

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001 年 8 月 2 日 (02.08.2001)

PCT

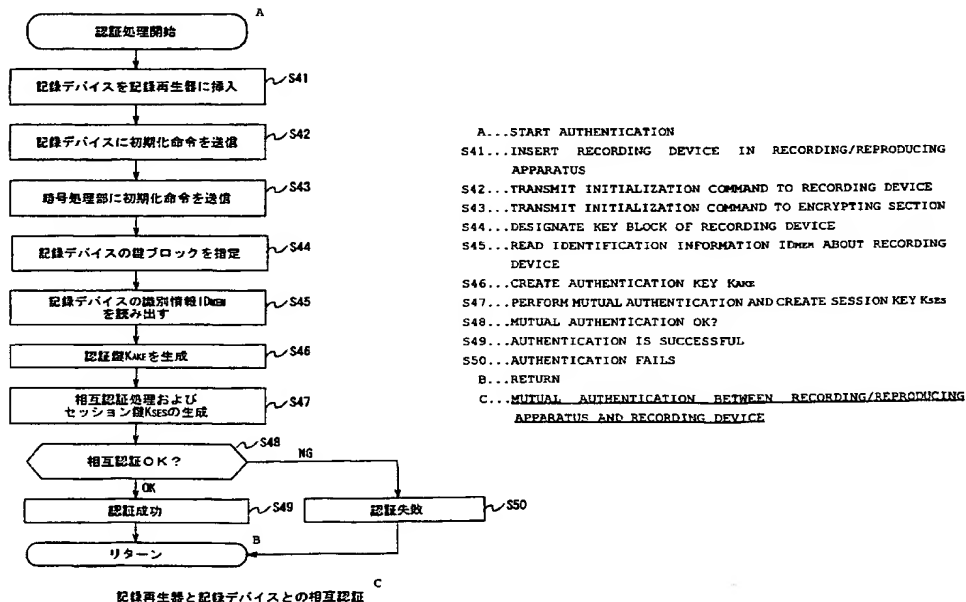
(10) 国際公開番号  
WO 01/56224 A1

- (51) 国際特許分類<sup>7</sup>: H04L 9/32, 9/08, G09C 1/00, G06F 12/14, 9/06
- (21) 国際出願番号: PCT/JP01/00526
- (22) 国際出願日: 2001 年 1 月 26 日 (26.01.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2000-16501 2000 年 1 月 26 日 (26.01.2000) JP  
特願2000-16545 2000 年 1 月 26 日 (26.01.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP). 株式会社 ソニー・コンピュータエンタテインメント (SONY COMPUTER ENTERTAINMENT INC.) [JP/JP]; 〒107-0052 東京都港区赤坂7丁目1番地1号 Tokyo (JP).
- (72) 発明者; および  
(75) 発明者/出願人 (米国についてののみ): 石橋義人 (ISHIBASHI, Yoshihito) [JP/JP]. 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 秋下 徹 (AKISHITA, Toru) [JP/JP]. 白井太三 (SHIRAI, Taizo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 吉森正治 (YOSHIMORI, Masaharu) [JP/JP]; 〒107-0052 東京都港区赤坂7丁目1番地1号 株式会社 ソニー・コンピュータエンタテインメント内 Tokyo (JP).
- (74) 代理人: 弁理士 田辺恵基 (TANABE, Shigemoto); 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンファンタジアビル5階 Tokyo (JP).
- (81) 指定国 (国内): AU, BR, CA, CN, KR, MX, NZ, RU, SG, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 添付公開書類:  
— 国際調査報告書

[続葉有]

(54) Title: STORAGE DEVICE AUTHENTICATION SYSTEM

(54) 発明の名称: 記憶デバイスの認証処理システム



(57) Abstract: To transfer data between a storage device and a recording/reproducing apparatus, key blocks where key data for authentication is stored are produced in the storage device, and the recording / reproducing apparatus designates one of the key blocks and performs authentication between them according to the key data stored in the designated key block.

[続葉有]

WO 01/56224 A1



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

記憶デバイスと記録再生器との間においてデータ転送を実行するにあたり、記憶デバイスに認証処理用の鍵データを格納した鍵ブロックを複数構成し、記録再生器は、記録デバイスとの間での認証処理において、前記鍵ブロックの1つを指定して該指定鍵ブロックに格納された鍵データに基づいて認証処理を実行する。

## 明 細 書

### 記憶デバイスの認証処理システム

#### 技術分野

本発明は、データ処理システム、記録デバイス、およびデータ処理方法、並びにプログラム提供媒体に関し、さらに詳細には、データ転送を実行する２つの装置間において、コンテンツの利用制限を考慮した装置間の認証処理を可能とする構成を実現するデータ処理システム、記録デバイス、データ処理方法に関し、また、データ転送を実行する２つの装置間において相互認証処理を必須要件として実行させ、認証処理の成立を条件としてコンテンツの利用を可能ならしめる構成を実現するデータ処理システム、記録デバイス、データ処理方法に関する。

本発明は、DVD、CD等の記憶媒体、あるいはCATV、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモ리카ード、ハードディスク、CD-R等に格納するとともに、記録デバイスに格納されたコンテンツを利用する際、コンテンツ配信側の希望する利用制限を付す構成を実現するとともに、この配布されたコンテンツを、正規ユーザ以外の第三者に不正利用されないようにセキュリティを確保する構成および方法に関する。

#### 背景技術

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して流通している。これらの流通コンテンツは、ユーザ

の所有するPC (Personal Computer)、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモ리카ード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。

従来のビデオゲーム機器、PC等の情報機器において使用されるメモ리카ード装置の主な構成要素は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモ리카ードに備えられた不揮発性メモリはEEPROM、フラッシュメモリ等によって構成される。

このようなメモ리카ードに記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により不揮発性メモリから呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ(平文)に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い

、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはRSA（Rivest-Shamir-Adleman）暗号がある。

このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザ

に対してのみ復号可能とするシステムが可能となる。これらの暗号方式を採用した従来のコンテンツ配布構成について図 1 を用いて簡単に説明する。

図 1 は、P C（パーソナルコンピュータ）、ゲーム機器等の再生手段 1 0 において、DVD、CD 3 0、インターネット 4 0 等のデータ提供手段から取得したプログラム、音声データ、映像データ等（コンテンツ（Content））を再生するとともに、DVD、CD 3 0、インターネット 4 0 等から取得したデータをフロッピーディスク、メモ리카ード、ハードディスク等の記憶手段 2 0 に記憶可能とした構成例を示すものである。

プログラム、音声データ、映像データ等のコンテンツは、暗号化処理がなされ、再生手段 1 0 を有するユーザに提供される。正規ユーザは、暗号化データとともに、その暗号化、復号化鍵である鍵データを取得する。

再生手段 1 0 は CPU 1 2 を有し、入力データの再生処理を再生処理部 1 4 で実行する。再生処理部 1 4 は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

正規ユーザは、提供されたプログラムを、再度使用するために記憶手段 2 0 にプログラム／データ等、コンテンツの保存処理を行なう。再生手段 1 0 には、このコンテンツ保存処理を実行するための保存処理部 1 3 を有する。保存処理部 1 3 は、記憶手段 2 0 に記憶されたデータの不正使用を防止するため、データに暗号化処理を施して保存処理を実行する。

コンテンツを暗号化する際には、コンテンツ暗号用鍵を用いる。保存処理部 1 3 は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それを F D（フロッピーディスク）、メモ리카ード、ハードディスク等の記憶手段 2 0 の記憶部 2 1 に記憶する。

ユーザは、記憶手段 2 0 から格納コンテンツを取り出して再生する場合には、記憶手段 2 0 から、暗号化データを取り出して、再生手段 1 0 の再生処理部 1 4 において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。

図 1 に示す従来の構成例に従えば、フロッピーディスク、メモ리카ード等の記憶手段 20 では格納コンテンツが暗号化されているため、外部からの不正読み出しは防止可能となる。しかしながら、このフロッピーディスクを他の PC、ゲーム機器等の情報機器の再生手段で再生して利用しようとする、同じコンテンツ鍵、すなわち暗号化されたコンテンツを復号するための同じ復号化鍵を有する再生手段でなければ再生不可能となる。従って、複数の情報機器において利用可能な形態を実現するためには、ユーザに提供する暗号鍵を共通化しておくことが必要となる。

しかしながら、コンテンツの暗号鍵を共通化するという事は、正規ライセンスを持たないユーザに暗号処理用の鍵を無秩序に流通させる可能性を高めることになり、正規のライセンスを持たないユーザによるコンテンツの不正利用を防止できなくなるという欠点があり、正規ライセンスを持たない PC、ゲーム機器等での不正利用の排除が困難になる。

さらに、上述のように鍵を共通化した環境においては、例えばある PC 上で作成され、メモ리카ード、フロッピーディスク等の記憶手段に保存された暗号化されたコンテンツは、別のフロッピーディスクに容易に複製することが可能であり、オリジナルのコンテンツデータではなく複製フロッピーディスクを用いた利用形態が可能となり、ゲーム機器、PC 等の情報機器において利用可能なコンテンツデータが多数複製されたり、または改竄されてしまう可能性があった。

コンテンツデータの利用を正当な利用者に限定する手法として認証処理があるが、従来の 2 装置間で実行される認証処理は、相互認証に用いる鍵、すなわち認証鍵を共通なものを使用して行なうのが一般的であった。従って、例えば製品仕向け先（国別）ごと、あるいは製品ごとに認証鍵を変更しようすると、記録再生器側と、記録デバイス側の認証処理に必要な鍵データを双方の機器において変更することが必要となる。

従って例えば新たに発売された記録再生器に格納された認証処理に必要な鍵データは、先に販売された記録デバイスに格納された認証処理に必要な鍵

データに対応せず、新たな記録再生器は、古いバージョンの記録デバイスへのアクセスができなくなってしまう事態が発生する。逆に新しいバージョンの記録デバイスと古いバージョンの記録再生器との関係においても同様の事態が発生する。

#### 発明の開示

本発明は、このような従来技術の問題点を解決するものであり、本発明の構成においては、予め記録デバイスに複数の異なる鍵セットとしての鍵ブロックが格納されている。記録再生器は例えば製品仕向け先（国別）ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロック、すなわち指定鍵ブロックが設定され、データ転送を実行する2つの装置間において、コンテンツの利用制限を考慮した装置間の認証処理、コンテンツの格納処理を可能とする。

さらに、認証処理と、コンテンツの利用処理とをいかに関連させるか、すなわち、認証処理の手続きをコンテンツの復号処理、または格納処理といかに密接不可分な手続きとして実行させるかについては明確な構成が実現されていない。認証処理についてもパスワードを用いたユーザ認証等は可能であるが記録再生器、あるいは記録デバイス等、機器に対する認証処理とコンテンツ利用処理とを関連付けてコンテンツの不正な利用を排除した構成は実現されていない。

従って例えば、異なる記録再生器において、パスワード入力等によって認証処理を実行すれば、複数の異なる機器においてもコンテンツが利用されてしまい、このようなコンテンツの流用を防止するためには、機器そのものに対する認証処理とコンテンツ利用処理とを関連付ける処理が必要となる。

本発明は、このような問題点を解決するものであり、本発明の構成においては、記録デバイスにおける認証処理、格納データの暗号処理等を所定のシーケンスにしたがって実行するように規定することにより、機器の認証の実行されていないコンテンツの外部装置からの読み出し等、コンテンツ利用を防止するデータ処

理システム、記録デバイス、およびデータ処理方法を提供する。

かかる課題を解決するため本発明の第1の側面は、相互に暗号データの転送を実行する記録再生器と記録デバイスとからなるデータ処理システムにおいて、上記記録デバイスは、記録再生器と記録デバイス間において転送可能なコンテンツデータを記憶するデータ記憶部を有するとともに、記録再生器と記録デバイス間の少なくとも認証処理に適用可能な鍵データを格納した鍵ブロックを複数有し、該複数の鍵ブロックに格納された鍵データは各ブロック毎に異なる鍵データを格納した構成を持ち、上記記録再生器は、記録再生器と記録デバイス間の認証処理において、上記記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して、指定鍵ブロックに格納された鍵データに基づいて上記記録デバイスとの認証処理を実行する構成を有することを特徴とするデータ処理システムにある。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスの複数の鍵ブロック各々には、少なくとも認証処理に適用可能な認証鍵を含み、各鍵ブロックの認証鍵は相互に異なる鍵データとして構成されていることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録再生器は、認証処理に適用すべき鍵ブロックを指定鍵ブロックとして設定した設定情報を記録再生器内メモリに保持し、上記記録再生器は、記録再生器と記録デバイス間の認証処理に際して記録再生器内メモリに保持された設定情報に基づいて上記記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して認証処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録再生器の指定鍵ブロック設定情報は、記録再生器の機種またはバージョンまたは出荷先等の所定製品単位毎に異なるように設定された構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録再生器は、上記記録デバイスとの認証処理に必要な認証処理用鍵データを記録再生器内

メモリに格納した構成を持ち、上記記録再生器内メモリに格納された認証処理用鍵データは、上記記録デバイスの複数の鍵ブロックの一部の鍵ブロックにのみ格納されたブロック内鍵データを使用した認証処理においてのみ認証が成立し、他の鍵ブロック内鍵データを用いた認証処理においては認証の成立しない鍵データであることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録再生器は、記録デバイス認証鍵用マスター鍵MK a k eを記録再生器内メモリに格納し、上記記録デバイス認証鍵用マスター鍵MK a k eに基づいて生成される認証鍵K a k eは、該記録再生器に設定された指定鍵ブロック内の鍵データを使用した認証処理においてのみ認証が成立し、他の鍵ブロック内鍵データを用いた認証処理においては認証の成立しない認証鍵であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスは、上記記録デバイス内メモリに記録デバイス識別情報ID m e mを有するとともに、上記複数の鍵ブロックの各々に鍵ブロック毎に異なる認証鍵K a k eを格納した構成を有し、上記記録再生器は、記録再生器内メモリに格納された記録デバイス認証鍵用マスター鍵MK a k eに基づく上記記録デバイス識別情報ID m e mの暗号処理によって認証鍵K a k eを生成し、該生成した認証鍵K a k eを用いて上記記録デバイスの指定鍵ブロックとの認証処理を行なう構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスの鍵ブロックの各々には、記録デバイスの固有情報である記録デバイス識別子情報、記録再生器間との認証処理において使用される認証鍵および乱数生成鍵、さらに上記データ記憶部への格納データの暗号化処理に用いられる保存鍵を含むことを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスの複数の鍵ブロックの各々に格納された上記保存鍵は、各鍵ブロック毎に異なる鍵データであるとともに上記データ記憶部の格納データに対する暗号処理に用

いられる鍵であり、上記記録デバイスは、記録デバイス外部から保存鍵で暗号化されたデータの利用要求があった場合は、記録デバイス内において保存鍵の鍵交換処理を実行して保存鍵と異なる鍵による暗号化データを記録デバイス外部に出力する構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスは、暗号処理部を有し、該暗号処理部は、上記記録再生器から受信する鍵ブロック指定情報に従って記録デバイスの複数の鍵ブロックの1つの鍵ブロックを選択し、該選択鍵ブロック内の鍵データを用いて上記記録再生器との認証処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスにおける暗号処理部は、記録再生器と記録デバイス間において転送可能なコンテンツデータを記憶したデータ記憶部に対するデータ格納処理およびデータ記憶部からのデータ転送処理において実行する暗号処理を上記記録再生器から受信する鍵ブロック指定情報に従って選択した1つの鍵ブロック内の鍵データを用いて実行する構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録再生器の指定可能な上記記録デバイスの鍵ブロックは複数であり、該複数の指定可能な鍵ブロック中の少なくとも1つの鍵ブロックは、他の記録再生器においても指定可能な共通指定可能な鍵ブロックとして構成されていることを特徴とする。

さらに、本発明の第2の側面は、外部装置との間で転送可能なコンテンツデータを記憶するデータ記憶部を有する記録デバイスであり、記録デバイスと上記外部装置間の少なくとも認証処理に適用可能な鍵データを格納した鍵ブロックを複数有し、該複数の鍵ブロックに格納された鍵データは各ブロック毎に異なる鍵データを格納した構成を有することを特徴とする記録デバイスにある。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスの複数の鍵ブロック各々には、少なくとも認証処理に適用可能な認証鍵を含み、各鍵ブロックの認証鍵は相互に異なる鍵データとして構成されていることを特徴とする。

る。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスは、上記記録デバイス内メモリに記録デバイス識別情報 I D m e m を有するとともに、上記複数の鍵ブロックの各々に鍵ブロック毎に異なる認証鍵 K a k e を格納した構成を有することを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスの鍵ブロックの各々には、記録デバイスの固有情報である記録デバイス識別子情報、上記外部装置との認証処理において使用される認証鍵および乱数生成鍵、さらに上記データ記憶部への格納データの暗号化処理に用いられる保存鍵を含むことを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスの複数の鍵ブロックの各々に格納された上記保存鍵は、各鍵ブロック毎に異なる鍵データであるとともに上記データ記憶部の格納データに対する暗号処理に用いられる鍵であり、上記記録デバイスは、記録デバイス外部から保存鍵で暗号化されたデータの利用要求があった場合は、記録デバイス内において保存鍵の鍵交換処理を実行して保存鍵と異なる鍵による暗号化データを記録デバイス外部に出力する構成を有することを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスは、暗号処理部を有し、該暗号処理部は、上記外部装置から受信する鍵ブロック指定情報に従って記録デバイスの複数の鍵ブロックの1つの鍵ブロックを選択し、該選択鍵ブロック内の鍵データを用いて上記記録再生器との認証処理を実行する構成を有することを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスにおける暗号処理部は、上記外部装置と記録デバイス間において転送可能なコンテンツデータを記憶したデータ記憶部に対するデータ格納処理およびデータ記憶部からのデータ転送処理において実行する暗号処理を上記外部装置から受信する鍵ブロック指定情報に従って選択した1つの鍵ブロック内の鍵データを用いて実行す

る構成を有することを特徴とする。

さらに、本発明の第3の側面は、相互に暗号データの転送を実行する記録再生器と記録デバイスとからなるデータ処理システムにおけるデータ処理方法において、記録再生器が、記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して、指定鍵ブロックに格納された鍵データに基づいて上記記録デバイスとの認証処理を実行することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記記録デバイスの複数の鍵ブロック各々には、少なくとも認証処理に適用可能な認証鍵を含み、各鍵ブロックの認証鍵は相互に異なる鍵データとして構成されていることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記記録再生器は、記録再生器と記録デバイス間の認証処理に際して記録再生器内メモリに保持された設定情報に基づいて上記記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して認証処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記記録再生器は、記録デバイス認証鍵用マスター鍵MKakeを記録再生器内メモリに格納し、上記記録デバイス認証鍵用マスター鍵MKakeに基づいて認証鍵Kakeを生成し、生成した認証鍵Kakeを用いて上記記録デバイスの有する複数の鍵ブロック中の指定鍵ブロック内の鍵データを使用した認証処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記記録デバイスは、上記記録デバイス内メモリに記録デバイス識別情報IDmemを有するとともに、上記複数の鍵ブロックの各々に鍵ブロック毎に異なる認証鍵Kakeを格納した構成を有し、上記記録再生器は、記録再生器内メモリに格納された記録デバイス認証鍵用マスター鍵MKakeに基づく上記記録デバイス識別情報IDmemの暗号処理を実行して認証鍵Kakeを生成し、生成した認証鍵Kakeを用いて上記記録デバイスの指定鍵ブロックとの認証処理を行なうことを特徴とする。

。

さらに、本発明のデータ処理方法の一実施態様において、上記記録デバイスは、上記記録再生器から受信する鍵ブロック指定情報に従って記録デバイスの複数の鍵ブロックの1つの鍵ブロックを選択し、該選択鍵ブロック内の鍵データを用いて上記記録再生器との認証処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、上記記録デバイスは、記録再生器と記録デバイス間において転送可能なコンテンツデータを記憶したデータ記憶部に対するデータ格納処理およびデータ記憶部からのデータ転送処理において実行する暗号処理を上記記録再生器から受信する鍵ブロック指定情報に従って選択した1つの鍵ブロック内の鍵データを用いて実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記記録デバイスの複数の鍵ブロックの各々には、上記記録デバイス内のデータ記憶部の格納データの暗号処理に用いられる保存鍵を含み、記録デバイス外部から保存鍵で暗号化されたデータの利用要求があった場合、記録デバイス内において保存鍵の鍵交換処理を実行して保存鍵と異なる鍵による暗号化データを記録デバイス外部に出力することを特徴とする。

さらに、本発明の第4の側面は、相互に暗号データの転送を実行する記録再生器と記録デバイスとからなるデータ処理システムにおけるデータ処理方法をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、記録再生器が、記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して、指定鍵ブロックに格納された鍵データに基づいて上記記録デバイスとの認証処理を実行するステップを含むことを特徴とするプログラム提供媒体にある。

本発明の第5の側面は、相互に暗号データの転送を実行する第1の装置と第2の装置とからなるデータ処理システムにおいて、上記第2の装置は、上記第1の装置との転送データに関する暗号処理を実行する暗号処理部を有し、該暗号処理

部は、上記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、該制御部は、上記第1の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とするデータ処理システムにある。

さらに、本発明のデータ処理システムの一実施態様において、上記制御部の有する上記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、上記制御部は、上記第1の装置からの受領コマンド番号の受付値をメモリに格納するとともに、上記第1の装置からの新規受領コマンド番号を、上記メモリに格納した受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行わず、上記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記第2の装置は、上記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、上記コマンドレジスタには、上記第1の装置と上記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、上記第1の装置と上記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、上記認証処理コマンドシーケンスに対応するコマンド識別子は、上記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記暗号処理コマンドシーケンスは、上記第1の装置から上記第2の装置に対して転送され、上記第2の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を

含むコマンドシーケンス、または、上記第 2 の装置内の記憶手段に格納され、上記第 2 の装置から上記第 1 の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記制御部は、上記第 1 の装置と上記第 2 の装置との認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、上記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、上記制御部は、上記認証処理コマンドシーケンスを新たに実行する際に上記認証フラグをリセットすることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記制御部は、上記暗号鍵交換処理において、上記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、上記制御部は、上記鍵交換処理に関する一連のコマンド実行中は、上記第 1 の装置を含む外部装置からの上記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記第 2 の装置は、暗号化データを記憶するデータ記憶部を有する記憶デバイスであり、上記第 1 の装置は、上記記憶デバイスに対するデータの格納処理、および上記記憶デバイスに格納されたデータを取り出して再生、実行を行なう記録再生器であり、上記記録再生器は、上記記録デバイスとの転送データの暗号処理を実行する暗号処理部を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記記録デバイスは、上記記録再生器と記録デバイス間の認証処理に適用する認証鍵、および上記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、上記記録デバイスの暗号処理部における上記制御部は、上記記録再生器から上記設定シーケンスにしたがってコマンド識別子を受領して上記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完

了後に上記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、上記記録再生器は、上記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する1つの鍵ブロックを指定鍵ブロックとして上記記録デバイスに通知し、上記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする。

さらに、本発明の第6の側面は、外部装置との間で転送可能なコンテンツデータを記憶するデータ記憶部を有する記録デバイスであり、上記記録デバイスは、外部装置との転送データに関する暗号処理を実行する暗号処理部を有し、該暗号処理部は、外部装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、該制御部は、上記外部装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とする記録デバイスにある。

さらに、本発明の記録デバイスの一実施態様において、上記制御部は、上記設定シーケンスとして、順次、番号がインクリメントされるコマンド番号設定シーケンスを有し、上記制御部は、上記外部装置からの受領コマンド番号の受付値をメモリに格納するとともに、上記外部装置からの新規受領コマンド番号を、上記メモリに格納した受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行わず、上記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスは、

上記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、上記コマンドレジスタには、上記外部装置と上記記録デバイスとの認証処理を実行する認証処理コマンドシーケンスと、上記外部装置と上記記録デバイスとの間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、上記認証処理コマンドシーケンスに対応するコマンド識別子は、上記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記暗号処理コマンドシーケンスは、上記外部装置から上記記録デバイスに対して転送され、上記記録デバイス内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、上記記録デバイス内の記憶手段に格納され、上記記録デバイスから上記外部装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記制御部は、上記外部装置と上記記録デバイスとの認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、上記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、上記制御部は、上記認証処理コマンドシーケンスを新たに実行する際に上記認証フラグをリセットすることを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記制御部は、上記暗号鍵交換処理において、上記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、上記制御部は、上記鍵交換処理に関する一連のコマンド実行中は、上記外部装置を含む外部装置からの上記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記記録デバイスは、上記外部装置と記録デバイス間の認証処理に適用する認証鍵、および上記記録デ

バイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、上記記録デバイスの暗号処理部における上記制御部は、上記外部装置から上記設定シーケンスにしたがってコマンド識別子を受領して上記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に上記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする。

さらに、本発明の記録デバイスの一実施態様において、上記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、上記外部装置は、上記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する1つの鍵ブロックを指定鍵ブロックとして上記記録デバイスに通知し、上記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする。

さらに、本発明の第7の側面は、相互に暗号データの転送を実行する第1の装置と第2の装置とからなるデータ処理システムにおけるデータ処理方法であり、上記第2の装置は、上記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを実行し、上記コマンド処理制御において、上記第1の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記コマンド処理制御ステップにおいて、上記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、上記コマンド処理制御ステップは、上記第1の装置からの受領コマンド番号の受付値をメモリに格納するステップと、上記第1の装置からの新規受領コマンド番号を、上記メモリに格納した受付済みコマンド番号に基づいて設定シー

ケンスとの一致を判定する判定ステップと、上記判定ステップにおいて、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行わず、上記メモリに格納したコマンド番号のリセットを実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、上記コマンド処理制御ステップは、上記第1の装置と上記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、上記第1の装置と上記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとを、実行するステップであり、上記設定シーケンスは、上記認証処理コマンドシーケンスを上記暗号処理コマンドシーケンスに先行して実行するシーケンスであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記暗号処理コマンドシーケンスは、上記第1の装置から上記第2の装置に対して転送され、上記第2の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、上記第2の装置内の記憶手段に格納され、上記第2の装置から上記第1の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記第1の装置と上記第2の装置との認証処理により認証が成立した場合に認証済みであることを示す認証フラグを設定する認証フラグ設定ステップを含み、上記コマンド処理制御ステップは、上記認証フラグが設定されている間は、上記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記認証処理コマンドシーケンスを新たに実行する際に上記認証フラグをリセットすることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法

における上記コマンド処理制御ステップにおいて、上記鍵交換処理に関する一連のコマンド実行中は、上記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

上記第1の装置を含む外部装置からの上記設定シーケンスと異なるコマンド処理を受け付けないことを特徴とする。

さらに、本発明の第8の側面は、相互に暗号データの転送を実行する第1の装置と第2の装置とからなるデータ処理システムにおけるデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記第1の装置から上記第2の装置に転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを有し、上記コマンド処理制御ステップにおいて、上記第1の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止するステップを含むことを特徴とするプログラム提供媒体にある。

本発明に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する

図面に基づくより詳細な説明によって明らかになるであろう。

このように、本発明のデータ処理システム、記録デバイス、およびデータ処理方法によれば、記録デバイスに認証処理に適用可能な鍵データを格納した鍵ブロックを複数構成し、複数の鍵ブロックに格納された鍵データを各ブロック毎に異なる鍵データとし、記録再生器と記録デバイス間の認証処理を特定の鍵ブロックを指定して実行するように構成したので、製品仕向け先（国別）ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロックを設定することで、製品、機種、バージョン、アプリケーションごとのコンテンツ利用制限を容易に設定することが可能となる。

さらに、本発明のデータ処理システム、記録デバイス、およびデータ処理方法によれば、各鍵ブロックに格納された保存鍵が異なる鍵によって構成されているので、異なる鍵ブロックで記録デバイスの記憶部に格納されたコンテンツデータ、あるいは鍵データ等は、他の鍵ブロックの設定がなされた記録再生器を利用した復号処理が不可能となるので、コンテンツデータ、あるいは鍵データの不正な流通を防止することが可能となる。

さらに、本発明のデータ処理システム、記録デバイス、およびデータ処理方法においては、記録デバイスにおける認証処理、および格納データの暗号処理等の各種処理を実行コマンド順を予め定めた設定シーケンスにしたがって実行するように構成した。すなわち、記録再生器から記録デバイスに対してコマンド番号を送信し、記録デバイスの制御部が予め定めたシーケンスにしたがったコマンド番号のみを受け付けて実行する構成とするとともに、設定シーケンスの認証処理コマンドを暗号処理コマンドに先行して実行するように設定したので、認証処理の済んだ記録再生器のみが記録デバイスに対するコンテンツの格納、または再生処理が実行でき、認証処理の済まない不正な機器によるコンテンツ利用が排除可能となる。

さらに、本発明のデータ処理システム、記録デバイス、およびデータ処理方法によれば、認証処理の済んだことを示す認証フラグを設定し、認証フラグの設定

された機器に対しては、暗号化データの格納処理、再生処理を実行可能としたので、格納処理、再生処理を繰り返し実行する場合、認証フラグが設定されている場合は、繰り返し認証処理を実行する必要がなく、効率的なデータ処理が可能となる。

#### 図面の簡単な説明

図 1 は、従来のデータ処理システムの構成を示す図である。

図 2 は、本発明の適用されるデータ処理装置の構成を示す図である。

図 3 は、本発明の適用されるデータ処理装置の構成を示す図である。

図 4 は、メディア上、通信路上におけるコンテンツデータのデータフォーマットを示す図である。

図 5 は、コンテンツデータ中のヘッダに含まれる取扱方針を示す図である。

図 6 は、コンテンツデータ中のヘッダに含まれるブロック情報を示す図である。

図 7 は、DES を用いた電子署名生成方法を示す図である。

図 8 は、トリプルDES を用いた電子署名生成方法を示す図である。

図 9 は、トリプルDES の態様を説明する図である。

図 10 は、一部にトリプルDES を用いた電子署名生成方法を示す図である。

図 11 は、電子署名生成における処理フローを示す図である。

図 12 は、電子署名検証における処理フローを示す図である。

図 13 は、対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

図 14 は、公開鍵証明書を説明する図である。

図 15 は、非対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

図 16 は、楕円曲線暗号を用いた暗号化処理の処理フローを示す図である。

図 17 は、楕円曲線暗号を用いた復号化処理の処理フローを示す図である。

図 1 8 は、記録再生器上のデータ保持状況を示す図である。

図 1 9 は、記録デバイス上のデータ保持状況を示す図である。

図 2 0 は、記録再生器と記録デバイスとの相互認証処理フローを示す図である。

図 2 1 は、記録再生器のマスタ鍵と記録デバイスの対応鍵ブロックとの関係を示す図である。

図 2 2 は、コンテンツのダウンロード処理における処理フローを示す図である。

図 2 3 は、チェック値 A : I C V a の生成方法を説明する図である。

図 2 4 は、チェック値 B : I C V b の生成方法を説明する図である。

図 2 5 は、総チェック値、記録再生器固有チェック値の生成方法を説明する図である。

図 2 6 は、記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報＝0）を示す図である。

図 2 7 は、記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報＝1）を示す図である。

図 2 8 は、コンテンツの再生処理における処理フローを示す図である。

図 2 9 は、記録デバイスにおけるコマンド実行方法について説明する図である。

図 3 0 は、記録デバイスにおけるコンテンツ格納処理におけるコマンド実行方法について説明する図である。

図 3 1 は、記録デバイスにおけるコンテンツ再生処理におけるコマンド実行方法について説明する図である。

図 3 2 は、コンテンツデータフォーマットのフォーマット・タイプ 0 の構成を説明する図である。

図 3 3 は、コンテンツデータフォーマットのフォーマット・タイプ 1 の構成を説明する図である。

図 3 4 は、コンテンツデータフォーマットのフォーマット・タイプ 2 の構成を説明する図である。

図 3 5 は、コンテンツデータフォーマットのフォーマット・タイプ 3 の構成を説明する図である。

図 3 6 は、フォーマット・タイプ 0 におけるコンテンツチェック値  $ICV_i$  の生成処理方法を説明する図である。

図 3 7 は、フォーマット・タイプ 1 におけるコンテンツチェック値  $ICV_i$  の生成処理方法を説明する図である。

図 3 8 は、フォーマット・タイプ 2, 3 における総チェック値、記録再生器固有チェック値の生成処理方法を説明する図である。

図 3 9 は、フォーマット・タイプ 0, 1 におけるコンテンツダウンロード処理の処理フローを示す図である。

図 4 0 は、フォーマット・タイプ 2 におけるコンテンツダウンロード処理の処理フローを示す図である。

図 4 1 は、フォーマット・タイプ 3 におけるコンテンツダウンロード処理の処理フローを示す図である。

図 4 2 は、フォーマット・タイプ 0 におけるコンテンツ再生処理の処理フローを示す図である。

図 4 3 は、フォーマット・タイプ 1 におけるコンテンツ再生処理の処理フローを示す図である。

図 4 4 は、フォーマット・タイプ 2 におけるコンテンツ再生処理の処理フローを示す図である。

図 4 5 は、フォーマット・タイプ 3 におけるコンテンツ再生処理の処理フローを示す図である。

図 4 6 は、コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図(その 1)である。

図 4 7 は、コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成

、検証方法を説明する図（その２）である。

図４８は、コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図（その３）である。

図４９は、マスタ鍵を用いて各種の鍵を個別に生成する方法について説明する図である。

図５０は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例１）である。

図５１は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例２）である。

図５２は、マスタ鍵の使い分けにより、利用制限を実行する構成について説明する図である。

図５３は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例３）である。

図５４は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例４）である。

図５５は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例５）である。

図５６は、トリプルDESを適用した暗号鍵をシングルDESアルゴリズムを用いて格納する処理フローを示す図である。

図５７は、優先順位に基づくコンテンツ再生処理フロー（例１）を示す図である。

図５８は、優先順位に基づくコンテンツ再生処理フロー（例２）を示す図である。

図５９は、優先順位に基づくコンテンツ再生処理フロー（例３）を示す図である。

図６０は、コンテンツ再生処理における圧縮データの復号（伸長）処理を実行する構成について説明する図である。

図 6 1 は、コンテンツの構成例（例 1）を示す図である。

図 6 2 は、コンテンツの構成例 1 における再生処理フローを示す図である。

図 6 3 は、コンテンツの構成例（例 2）を示す図である。

図 6 4 は、コンテンツの構成例 2 における再生処理フローを示す図である。

図 6 5 は、コンテンツの構成例（例 3）を示す図である。

図 6 6 は、コンテンツの構成例 3 における再生処理フローを示す図である。

図 6 7 は、コンテンツの構成例（例 4）を示す図である。

図 6 8 は、コンテンツの構成例 4 における再生処理フローを示す図である。

図 6 9 は、セーブデータの生成、格納処理について説明する図である。

図 7 0 は、セーブデータの格納処理例（例 1）に関する処理フローを示す図である。

図 7 1 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（例 1）を示す図である。

図 7 2 は、セーブデータの再生処理例（例 1）に関する処理フローを示す図である。

図 7 3 は、セーブデータの格納処理例（例 2）に関する処理フローを示す図である。

図 7 4 は、セーブデータの再生処理例（例 2）に関する処理フローを示す図である。

図 7 5 は、セーブデータの格納処理例（例 3）に関する処理フローを示す図である。

図 7 6 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（例 2）を示す図である。

図 7 7 は、セーブデータの再生処理例（例 3）に関する処理フローを示す図である。

図 7 8 は、セーブデータの格納処理例（例 4）に関する処理フローを示す図である。

図 7 9 は、セーブデータの再生処理例(例 4)に関する処理フローを示す図である。

図 8 0 は、セーブデータの格納処理例(例 5)に関する処理フローを示す図である。

図 8 1 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例 3)を示す図である。

図 8 2 は、セーブデータの再生処理例(例 5)に関する処理フローを示す図である。

図 8 3 は、セーブデータの格納処理例(例 6)に関する処理フローを示す図である。

図 8 4 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例 4)を示す図である。

図 8 5 は、セーブデータの再生処理例(例 6)に関する処理フローを示す図である。

図 8 6 は、コンテンツ不正利用者排除(リボケーション)構成を説明する図である。

図 8 7 は、コンテンツ不正利用者排除(リボケーション)の処理フロー(例 1)を示す図である。

図 8 8 は、コンテンツ不正利用者排除(リボケーション)の処理フロー(例 2)を示す図である。

図 8 9 は、セキュリティチップの構成(例 1)を説明する図である。

図 9 0 は、セキュリティチップの製造方法における処理フローを示す図である。

図 9 1 は、セキュリティチップの構成(例 2)を説明する図である。

図 9 2 は、セキュリティチップ(例 2)におけるデータ書き込み処理における処理フローを示す図である。

図 9 3 は、セキュリティチップ(例 2)における書き込みデータチェック処理

における処理フローを示す図である。

発明を実施するための最良の形態

以下に本発明の実施の形態を説明する。説明の手順は、以下の項目に従って行なう。

- (1) データ処理装置構成
- (2) コンテンツデータフォーマット
- (3) データ処理装置において適用可能な暗号処理概要
- (4) 記録再生器の格納データ構成
- (5) 記録デバイスの格納データ構成
- (6) 記録再生器、記録デバイス間における相互認証処理
  - (6-1) 相互認証処理の概要
  - (6-2) 相互認証時の鍵ブロックの切り替え
- (7) 記録再生器から記録デバイスへのダウンロード処理
- (8) 記録デバイス格納情報の記録再生器での再生処理
- (9) 相互認証後の鍵交換処理
- (10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理
  - (11) コンテンツプロバイダにおけるチェック値 (ICV) 生成処理態様
  - (12) マスタ鍵に基づく暗号処理鍵生成構成
  - (13) 暗号処理における暗号強度の制御
  - (14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理
- (15) コンテンツ構成および再生(伸長)処理
- (16) セーブデータの生成および記録デバイスへの格納、再生処理
- (17) 不正機器の排除(リボケーション)構成
- (18) セキュアチップ構成および製造方法

### (1) データ処理装置構成

図2に本発明のデータ処理装置の一実施例に係る全体構成ブロック図を示す。本発明のデータ処理装置は、記録再生器300と記録デバイス400とを主要構成要素とする。

記録再生器300は、例えばパーソナル・コンピュータ（PC：Personal Computer）、あるいはゲーム機器等によって構成される。記録再生器300は、図2に示すように、記録再生器300における暗号処理時の記録デバイス400との通信制御を含む統括的制御を実行する制御部301、暗号処理全般を司る記録再生器暗号処理部302、記録再生器に接続される記録デバイス400と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ303、DVDなどのメディア500から少なくともデータの読み出しを行う読み取り部304、外部とデータの送受信を行う通信部305を有する。

記録再生器300は、制御部301の制御により記録デバイス400に対するコンテンツデータのダウンロード、記録デバイス400からのコンテンツデータ再生を実行する。記録デバイス400は、記録再生器300に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、EEPROM、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきRAMなどによって構成される外部メモリ402を有する。

記録再生器300は、図2の左端に示す記憶媒体、DVD、CD、FD、HDDに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部304、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部305を有し、外部からコンテンツを入力する。

記録再生器300は、暗号処理部302を有し、読取部304または通信部305を介して外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいはコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化处理、復号化处理、さらにデータの検証処理等

を実行する。暗号処理部 302 は、暗号処理部 302 全体を制御する制御部 306、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ 307、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部 308 から構成されている。

制御部 301 は、例えば、記録再生器 300 に記録デバイス 400 が装着された際に記録デバイスコントローラ 303 を介して記録デバイス 400 に初期化命令を送信したり、あるいは、記録再生器暗号処理部 302 の暗号／復号化部 308 と記録デバイス暗号処理部 401 の暗号／復号化部 406 の間で行われる相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。これらの各処理については、後段で詳細に説明する。

暗号処理部 302 は、前述のように認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、暗号処理制御部 306、内部メモリ 307、暗号／復号化部 308 を有する。

暗号処理制御部 306 は、記録再生器 300 において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、記録再生器 300 と記録デバイス 400 との間で実行される認証処理の完了時における認証完了フラグの設定、記録再生器暗号処理部 302 の暗号／復号化部 308 において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

内部メモリ 307 は、後段で詳細に説明するが、記録再生器 300 において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等を格納する。

暗号／復号化部 308 は、内部メモリ 307 に格納された鍵データ等を使用して、外部から入力されるコンテンツデータを記録デバイス 400 にダウンロード処理する際、あるいは記録デバイス 400 に格納されたコンテンツデータを記録

デバイス400から再生、実行する際の認証処理、暗号化处理、復号化处理、さらに所定のチェック値や電子署名の生成・検証、データの検証、乱数の発生などの処理を実行する。

ここで、記録再生器暗号処理部302の内部メモリ307は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部302は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。この構成については、後段で詳細に説明する。

記録再生器300は、これらの暗号処理機能の他に、中央演算処理装置（メインCPU: Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108、AV処理部109、入力インタフェース110、PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112を備えている。

中央演算処理装置（メインCPU: Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108は、記録再生器300本体の制御系として機能する構成部であり、主として記録再生器暗号処理部302で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインCPU: Central Processing Unit）106は、制御部301の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをAV処理部109へ出力する等、コンテンツの再生、実行に関する制御を行なう。

RAM107は、CPU106における各種処理用の主記憶メモリとして使用

され、メインCPU106による処理のための作業領域として使用される。ROM108は、メインCPU106で起動されるOS等を立ち上げるための基本プログラム等が格納される。

AV処理部109は、具体的には、例えばMPEG2デコーダ、ATRACデコーダ、MP3デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

入力インタフェース110は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインCPU106に出力する。メインCPU106は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112は、メモ리카ード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

また、メインCPU106は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス400に記憶する際の制御も行なう。この処理の際には、記憶データを制御部301に転送し、制御部301は必要に応じて暗号処理部302にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス400に格納する。これらの暗号処理については、後段で詳細に説明する。

記録デバイス400は、前述したように好ましくは記録再生器300に対して着脱可能な記憶媒体であり、例えばメモ리카ードによって構成される。記録デバイス400は暗号処理部401、外部メモリ402を有する。

記録デバイス暗号処理部401は、記録再生器300からのコンテンツデータのダウンロード、または記録デバイス400から記録再生器300へのコンテンツデータの再生処理時等における記録再生器300と記録デバイス400間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処

理部であり、記録再生器 300 の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。これらの詳細は図 3 に示す。外部メモリ 402 は、前述したように、例えば EEPROM 等のフラッシュメモリからなる不揮発メモリ、ハードディスク、電池つき RAM などによって構成され、暗号化されたコンテンツデータ等を格納する。

図 3 は、本発明のデータ処理装置がデータ供給を受けるコンテンツ提供手段であるメディア 500、通信手段 600 から入力されるデータ構成の概略を示すとともに、これらコンテンツ提供手段 500、600 からコンテンツを入力する記録再生器 300 と、記録デバイス 400 における暗号処理に関する構成を中心として、その構成を示した図である。

メディア 500 は、例えば光ディスクメディア、磁気ディスクメディア、磁気テープメディア、半導体メディア等である。通信手段 600 は、インターネット通信、ケーブル通信、衛星通信等の、データ通信可能な手段である。

図 3 において、記録再生器 300 は、コンテンツ提供手段であるメディア 500、通信手段 600 から入力されるデータ、すなわち図 3 に示すような所定のフォーマットに従ったコンテンツを検証し、検証後にコンテンツを記録デバイス 400 に保存する。

図 3 のメディア 500、通信手段 600 部分に示すようにコンテンツデータは以下のような構成部を有する。

識別情報：コンテンツデータの識別子としての識別情報。

取扱方針：コンテンツデータの構成情報、例えばコンテンツデータを構成するヘッダー部サイズ、コンテンツ部サイズ、フォーマットのバージョン、コンテンツがプログラムかデータか等を示すコンテンツタイプ、さらにコンテンツがダウンロードした機器だけでしか利用できないのか他の機器でも利用できるのか等の利用制限情報等を含む取扱方針。

ブロック情報：コンテンツブロックの数、ブロックサイズ、暗号化の有無を示す暗号化フラグ等から構成されるブロック情報。

鍵データ：上述のブロック情報を暗号化する暗号化鍵、あるいはコンテンツブロックを暗号化するコンテンツ鍵等からなる鍵データ。

コンテンツブロック：実際の再生対象となるプログラムデータ、音楽、画像データ等からなるコンテンツブロック。

を有する。なお、コンテンツデータ詳細については、後段で図4以下を用いてさらに詳細に説明する。

コンテンツデータは、コンテンツ鍵（ここでは、これをコンテンツ鍵（Content Key（以下、Kconとする））と呼ぶ）によって暗号化されて、メディア500、通信手段600から記録再生器300に提供される。コンテンツは、記録再生器300を介して記録デバイス400の外部メモリに格納することができる。

例えば、記録デバイス400は、記録デバイス内の内部メモリ405に格納された記録デバイス固有の鍵（ここでは、これを保存鍵（Storage Key（以下、Kstrとする））と呼ぶ）を用いて、コンテンツデータに含まれるコンテンツ、及びコンテンツデータのヘッダ情報として含まれるブロック情報、各種鍵情報、例えばコンテンツ鍵Kconなどを暗号化して外部メモリ402に記憶する。コンテンツデータの記録再生器300から記録デバイス400へのダウンロード処理、あるいは記録再生器300による記録デバイス400内に格納されたコンテンツデータの再生処理においては、機器間の相互認証処理、コンテンツデータの暗号化、復号化処理等、所定の手続きが必要となる。これらの処理については、後段で詳細に説明する。

記録デバイス400は、図3に示すように暗号処理部401、外部メモリ402を有し、暗号処理部401は、制御部403、通信部404、内部メモリ405、暗号／復号化部406、外部メモリ制御部407を有する。

記録デバイス400は、暗号処理全般を司り、外部メモリ402を制御するとともに、記録再生器300からのコマンドを解釈し、処理を実行する記録デバイス暗号処理部401と、コンテンツなどを保持する外部メモリ402からなる。

記録デバイス暗号処理部 401 は、記録デバイス暗号処理部 401 全体を制御する制御部 403、記録再生器 300 とデータの送受信を行う通信部 404、暗号処理用の鍵データなどの情報を保持し、外部から容易に読み出せないように処理が施された内部メモリ 405、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部 406、外部メモリ 402 のデータを読み書きする外部メモリ制御部 407 を有する。

制御部 403 は、記録デバイス 400 において実行される認証処理、暗号化／復号化処理等の暗号処理全般に係る制御を実行する制御部であり、例えば、記録再生器 300 と記録デバイス 400 との間で実行される認証処理の完了時における認証完了フラグの設定、暗号処理部 401 の暗号／復号化部 406 において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

内部メモリ 405 は、後段で詳細に説明するが、複数のブロックを持つメモリによって構成されており、記録デバイス 400 において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等の組を複数格納した構成となっている。

記録デバイス暗号処理部 401 の内部メモリ 405 は、先に説明した記録再生器暗号処理部 302 の内部メモリ 307 と同様、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録デバイス 400 の暗号処理部 401 は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされる。なお、記録再生器暗号処理部 302 は、鍵などの秘密の情報を容易に外部に漏らさないように構成されたソフトウェアであってもよい。

暗号／復号化部 406 は、記録再生器 300 からのコンテンツデータのダウン

ロード処理、記録デバイス400の外部メモリ402に格納されたコンテンツデータの再生処理、あるいは、記録再生器300と記録デバイス400間の相互認証処理の際、内部メモリ405に格納された鍵データ等を使用して、データの検証処理、暗号化処理、復号化処理、所定のチェック値や電子署名の生成・検証、乱数の発生などの処理等を実行する。

通信部404は、記録再生器300の記録デバイスコントローラ303に接続され、記録再生器300の制御部301、あるいは、記録デバイス403の制御部403の制御に従って、コンテンツデータのダウンロード処理、再生処理、あるいは、相互認証処理の際の記録再生器300と記録デバイス400間の転送データの通信を行なう。

## (2) コンテンツデータフォーマット

次に、図4乃至図6を用いて、本発明のシステムにおけるメディア500に格納され、またはデータ通信手段600上を流通するデータのデータフォーマットについて説明する。

図4に示す構成がコンテンツデータ全体のフォーマットを示す図であり、図5に示す構成がコンテンツデータのヘッダ部の一部を構成する「取扱方針」の詳細を示す図であり、図6に示す構成がコンテンツデータのヘッダ部の一部を構成する「ブロック情報」の詳細を示す図である。

なお、ここでは、本発明のシステムにおいて適用されるデータフォーマットの代表的な一例について説明するが、本発明のシステムでは、例えばゲームプログラムに対応したフォーマット、音楽データ等のリアルタイム処理に適したフォーマット等、異なる複数のデータフォーマットが利用可能であり、これらのフォーマットの態様については、後段「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」において、さらに詳しく述べる。

図4に示すデータフォーマットにおいて、グレーで示す部分は暗号化されたデータであり、二重枠の部分は改竄チェックデータ、その他の白い部分は暗号化さ

れていない平文のデータである。暗号化部の暗号化鍵は、それぞれの枠の左に示す鍵である。図4に示す例においては、コンテンツ部の各ブロック（コンテンツブロックデータ）に暗号化されたものと暗号化されていないものとが混在している。これらの形態は、コンテンツデータに応じて異なるものであり、データに含まれるすべてのコンテンツブロックデータが暗号化されている構成であってもよい。

図4に示すように、データフォーマットは、ヘッダー部とコンテンツ部に分かれており、ヘッダー部は、識別情報（Content ID）、取扱方針（Usage Policy）、チェック値A（Integrity Check Value A（以下、ICVaとする））、ブロック情報鍵（Block Information Table Key（以下、Kbitとする））、コンテンツ鍵Kcon、ブロック情報（Block Information Table（以下、BITとする））、チェック値B（ICVb）、総チェック値（ICVt）により構成されており、コンテンツ部は、複数のコンテンツブロック（例えば暗号化されたコンテンツと、暗号化されていないコンテンツ）から構成されている。

ここで、識別情報は、コンテンツを識別するための個別の識別子（Content ID）を示している。取扱方針は、図5にその詳細を示すように、ヘッダー部分のサイズを示すヘッダーサイズ（Header Length）、コンテンツ部分のサイズを示すコンテンツサイズ（Content Length）、フォーマットのバージョン情報を示すフォーマットバージョン（Format Version）、フォーマットの種類を示すフォーマットタイプ（Format Type）、コンテンツ部に保存されているコンテンツがプログラムなのか、データなのか等コンテンツの種類を示すコンテンツタイプ（Content Type）、コンテンツタイプがプログラムである場合の起動優先順位を示す起動優先順位情報（Operation Priority）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器だ

けでしか利用できないのか、他の同様な機器でも利用できるのかを示す利用制限情報 (Localization Field)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に複製できるのか否かを示す複製制限情報 (Copy Permission)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に移動できるのか否かを示す移動制限情報 (Move Permission)、コンテンツ部内のコンテンツブロックを暗号するのに使用したアルゴリズムを示す暗号アルゴリズム (Encryption Algorithm)、コンテンツ部内のコンテンツを暗号化するのに使用したアルゴリズムの使用方法を示す暗号化モード (Encryption Mode)、チェック値の生成方法を示す検証方法 (Integrity Check Method) から構成されている。

なお、上述した取扱方針に記録するデータ項目は、1つの例であり、対応するコンテンツデータの態様に応じて様々な取扱方針情報を記録することが可能である。例えば後段の「(17) 不正機器の排除 (リボケーション) 構成」で詳しく述べるが、不正な記録再生器の識別子をデータとして記録して、利用開始時の照合によって不正機器によるコンテンツ利用を排除するように構成することも可能である。

チェック値A、ICV aは、識別情報、取扱方針の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。データブロック情報鍵K b i tは、ブロック情報を暗号化するのに用いられ、コンテンツ鍵K c o nは、コンテンツブロックを暗号化するのに用いられる。なお、ブロック情報鍵K b i t及びコンテンツ鍵K c o nは、メディア500上および通信手段600上では後述する配送鍵 (Distribution Key (以下、K d i sとする)) で暗号化されている。

ブロック情報の詳細を図6に示す。なお、図6のブロック情報は、図4から理

解されるようにすべてブロック情報鍵  $K_{bit}$  によって暗号化されているデータである。ブロック情報は、図 6 に示すように、コンテンツブロックの数を示すコンテンツブロック数 ( $Block\ Number$ ) と  $N$  個のコンテンツブロック情報から構成されている。コンテンツブロック情報は、ブロックサイズ ( $Block\ Length$ )、暗号化されているか否かを示す暗号化フラグ ( $Encryption\ Flag$ )、チェック値を計算する必要があるか否かを示す検証対象フラグ ( $ICV\ Flag$ )、コンテンツチェック値 ( $ICV_i$ ) から構成されている。

コンテンツチェック値は、各コンテンツブロックの改竄を検証するために用いられるチェック値である。コンテンツチェック値の生成手法の具体例については、後段の「(10) 複数のデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理」の欄で説明する。なお、ブロック情報を暗号化しているブロック情報鍵  $K_{bit}$  は、さらに、配送鍵  $K_{dis}$  によって暗号化されている。

図 4 のデータフォーマットの説明を続ける。チェック値  $B$ 、 $ICV_b$  は、ブロック情報鍵  $K_{bit}$ 、コンテンツ鍵  $K_{con}$ 、ブロック情報の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。総チェック値  $ICV_t$  は、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値  $ICV_i$  (設定されている場合)、これらの部分チェック値、あるいはそのチェック対象となるデータ全ての改竄を検証するためのチェック値である。

なお、図 6 においては、ブロックサイズ、暗号化フラグ、検証対象フラグを自由に設定できるようにしているが、ある程度ルールを決めた構成としてもよい。例えば、暗号文領域と平文領域を固定サイズ繰り返しにしたり、全コンテンツデータを暗号化したりし、ブロック情報  $BIT$  を圧縮してもよい。また、コンテンツ鍵  $K_{con}$  をコンテンツブロック毎に異なるようにするため、コンテンツ鍵  $K_{con}$  をヘッダー部分ではなく、コンテンツブロックに含ませるようにしてもよ

い。コンテンツデータフォーマットの例については、「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」の項目において、さらに詳細に説明する。

### (3) 本発明のデータ処理装置において適用可能な暗号処理概要

次に、本発明のデータ処理装置において適用され得る各種暗号処理の態様について説明する。なお、本項目「(3) 本発明のデータ処理装置において適用可能な暗号処理の概要」に示す暗号処理に関する説明は、後段で具体的に説明する本発明のデータ処理装置における各種処理、例えば a. 記録再生器と記録デバイス間での認証処理。 b. コンテンツの記録デバイスに対するダウンロード処理。 c. 記録デバイスに格納したコンテンツの再生処理等の処理において実行される処理の基礎となる暗号処理の態様について、その概要を説明するものである。記録再生器 300 と記録デバイス 400 における具体的処理については、本明細書の項目 (4) 以下において、各処理毎に詳細に説明する。

以下、データ処理装置において適用可能な暗号処理の概要について、

- (3-1) 共通鍵暗号方式によるメッセージ認証
- (3-2) 公開鍵暗号方式による電子署名
- (3-3) 公開鍵暗号方式による電子署名の検証
- (3-4) 共通鍵暗号方式による相互認証
- (3-5) 公開鍵証明書
- (3-6) 公開鍵暗号方式による相互認証
- (3-7) 楕円曲線暗号を用いた暗号化处理
- (3-8) 楕円曲線暗号を用いた復号化处理
- (3-9) 乱数生成処理

の順に説明する。

#### (3-1) 共通鍵暗号方式によるメッセージ認証

まず、共通鍵暗号方式を用いた改竄検出データの生成処理について説明する。改竄検出データは、改竄の検出を行ないたいデータに付け、改竄のチェックおよ

び作成者認証をするためのデータである。

例えば、図4で説明したデータ構造中の二重枠部分の各チェック値A、B、総チェック値、および図6に示すブロック情報中の各ブロックに格納されたコンテンツチェック値等が、この改竄検出データとして生成される。

ここでは、電子署名データの生成処理方法の例の1つとして共通鍵暗号方式におけるDESを用いた例を説明する。なお、本発明においては、DES以外にも、同様の共通鍵暗号方式における処理として例えばFEAL (Fast Encryption Algorithm: NTT)、AES (Advanced Encryption Standard: 米国次期標準暗号) 等を用いることも可能である。

一般的なDESを用いた電子署名の生成方法を図7を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを8バイト単位に分割する(以下、分割されたメッセージをM1、M2、・・・、MNとする)。そして、初期値 (Initial Value (以下、IVとする)) とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENが電子署名になる。この値は一般にはメッセージ認証符号 (MAC (Message Authentication Code)) と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをCBC (Cipher Block Chaining) モードと呼ぶ。

なお、図7のような生成例において出力されるMAC値が、図4で示すデータ構造中の二重枠部分の各チェック値A、B、総チェック値、および図6に示すブロック情報中の各ブロックに格納されたコンテンツチェック値ICV1～ICVNとして使用可能である。このMAC値の検証時には、検証者が生成時と同様の

方法でMAC値を生成し、同一の値が得られた場合、検証成功とする。

なお、図7に示す例では初期値IVを、初めの8バイトメッセージM1に排他的論理和したが、初期値IV=0として、初期値を排他的論理和しない構成とすることも可能である。

図7に示すMAC値生成方法に対して、さらにセキュリティを向上させたMAC値生成方法を示す処理構成図を図8に示す。図8は、図7のシングルDESに代えてトリプルDES (Triple DES) を用いてMAC値の生成を実行する例を示したものである。

図8に示す各トリプルDES (Triple DES) 構成部の詳細構成例を図9に示す。図9(a)、(b)に示すようにトリプルDES (Triple DES) としての構成には2つの異なる態様がある。図9(a)は、2つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による復号化処理、さらに鍵1による暗号化処理の順に処理を行う。鍵は、K1、K2、K1の順に2種類用いる。図9(b)は3つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による暗号化処理、さらに鍵3による暗号化処理の順に処理を行い3回とも暗号化処理を行う。鍵は、K1、K2、K3の順に3種類の鍵を用いる。このように複数の処理を連続させる構成とすることで、シングルDESに比較してセキュリティ強度を向上させている。しかしながら、このトリプルDES (Triple DES) 構成は、処理時間がシングルDESのおよそ3倍かかるという欠点を有する。

図8および図9で説明したトリプルDES構成を改良したMAC値生成構成例を図10に示す。図10においては、署名対象となるメッセージ列の初めから途中までの各メッセージに対する暗号化処理は全てシングルDESによる処理とし、最後のメッセージに対する暗号化処理のみを図9(a)に示すトリプルDES (Triple DES) 構成としたものである。

図10に示すこのような構成とすることで、メッセージのMAC値の生成処理時間は、シングルDESによるMAC値生成処理に要する時間とほぼ同程度に短

縮され、かつセキュリティはシングルDESによるMAC値よりも高めることが可能となる。なお、最終メッセージに対するトリプルDES構成は、図9(b)の構成とすることも可能である。

### (3-2) 公開鍵暗号方式による電子署名

以上は、暗号化方式として共通鍵暗号化方式を適用した場合の電子署名データの生成方法であるが、次に、暗号化方式として公開鍵暗号方式を用いた電子署名の生成方法を図11を用いて説明する。図11に示す処理は、ECDSA ( ( Elliptic Curve Digital Signature Algorithm ) 、 IEEE P1363/D3 ) を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 ( Elliptic Curve Cryptography (以下、ECCと呼ぶ) ) を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばRSA暗号 ( ( Rivest, Shamir, Adleman ) など ( ANSI X9.31 ) ) を用いることも可能である。

図11の各ステップについて説明する。ステップS1において、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数 (楕円曲線:  $y^2 = x^3 + ax + b$ )、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $K_s$ を秘密鍵 ( $0 < K_s < r$ ) とする。ステップS2において、メッセージ $M$ のハッシュ値を計算し、 $f = \text{Hash}(M)$  とする。

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、図7他で説明したと同様のDES-CBCが用いられる場合もある。この場合は、最終出

力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

続けて、ステップS3で、乱数 $u$ （ $0 < u < r$ ）を生成し、ステップS4でベースポイントを $u$ 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

$P = (X_a, Y_a)$ ,  $Q = (X_b, Y_b)$ ,  $R = (X_c, Y_c) = P + Q$ とすると、

$P \neq Q$ のとき、（加算）、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P = Q$ の時（2倍算）、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a) \quad \dots\dots (1)$$

これらを用いて点 $G$ の $u$ 倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。 $G$ 、 $2 \times G$ 、 $4 \times G \dots$ を計算し、 $u$ を2進数展開して1が立っているところに対応する $2^i \times G$ （ $G$ を $i$ 回2倍算した値）を加算する（ $i$ は $u$ のLSBから数えた時のビット位置））。

ステップS5で、 $c = X_v \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cK_s) / u] \bmod r$ を計算し、ステップS8で $d$ が0であるかどうか判定し、 $d$ が0でなければ、ステップS9で $c$ および $d$ を電子署名データとして出力する。仮に、 $r$ を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

ステップS6において、 $c$ が0であった場合、ステップS3に戻って新たな乱

数を生成し直す。同様に、ステップS 8でdが0であった場合も、ステップS 3に戻って乱数を生成し直す。

### (3-3) 公開鍵暗号方式による電子署名の検証

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図12を用いて説明する。ステップS 11で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、Gおよび $K_s \times G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS 12で電子署名データcおよびdが $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS 13で、メッセージMのハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。次に、ステップS 14で $h = 1/d \bmod r$ を計算し、ステップS 15で $h_1 = fh \bmod r$ 、 $h_2 = ch \bmod r$ を計算する。

ステップS 16において、既に計算した $h_1$ および $h_2$ を用い、点 $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$ を計算する。電子署名検証者は、公開鍵Gおよび $K_s \times G$ を知っているので、図11のステップS 4と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップS 17で点Pが無限遠点かどうか判定し、無限遠点でなければステップS 18に進む（実際には、無限遠点の判定はステップS 16でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 $\lambda$ が計算できず、 $P + Q$ が無限遠点であることが判明している）。ステップS 18で $X_p \bmod r$ を計算し、電子署名データcと比較する。最後に、この値が一致していた場合、ステップS 19に進み、電子署名が正しいと判定する。

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

ステップS 12において、電子署名データcまたはdが、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップS 20に進む。また、ステップS 17において、点Pが無限遠点であった場合もステップS 20に進む。さらにまた、ステ

ップS18において、 $Xp \bmod r$ の値が、電子署名データcと一致していなかった場合にもステップS20に進む。

ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

### (3-4) 共通鍵暗号方式による相互認証

次に、共通鍵暗号方式を用いた相互認証方法を、図13を用いて説明する。図13において、共通鍵暗号方式としてDESを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図13において、まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Kabを用いてデータを暗号化し、Bに返送する。図7に示すDESのCBCモード処理構成によれば、RaがM1、RbがM2、ID(b)がM3に相当し、初期値：IV=0としたときの出力E1、E2、E3が暗号文となる。

これを受信したBは、受信データを鍵Kabで復号化する。受信データの復号化方法は、まず、暗号文E1を鍵Kabで復号化し、乱数Raを得る。次に、暗号文E2を鍵Kabで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を鍵Kabで復号化し、その結果とE2を排他的論理和し、ID(b)を得る。こうして得られたRa、Rb、ID(b)の内、RbおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

次にBは、認証後に使用するセッション鍵 (Session Key (以下、Ksesとする)) を生成する (生成方法は、乱数を用いる)。そして、Rb、Ra、Ksesの順に、DESのCBCモードで鍵Kabを用いて暗号化し、Aに返送する。

これを受信したAは、受信データを鍵Kabで復号化する。受信データの復号

化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた $R_b$ 、 $R_a$ 、 $K_{ses}$ の内、 $R_b$ および $R_a$ が、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵 $K_{ses}$ は、認証後の秘密通信のための共通鍵として利用される。

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

### (3-5) 公開鍵証明書

次に、公開鍵証明書について図14を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局(CA: Certificate Authority)が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

図14に示す公開鍵証明書は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前(ユーザID)、証明書利用者の公開鍵並びに電子署名を含む。

電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図11で説明した処理フローが適用される。

認証局は、図14に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布(これをリボケーション: Revocationと呼ぶ)を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図 1 2 で説明したのでその詳細は省略する。

### (3-6) 公開鍵暗号方式による相互認証

次に、公開鍵暗号方式である 160 ビット長の楕円曲線暗号を用いた相互認証方法を、図 1 5 を用いて説明する。図 1 5 において、公開鍵暗号方式として ECC を用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも 160 ビットでなくてもよい。図 1 5 において、まず B が、64 ビットの乱数  $R_b$  を生成し、A に送信する。これを受信した A は、新たに 64 ビットの乱数  $R_a$  および標数  $p$  より小さい乱数  $A_k$  を生成する。そして、ベースポイント  $G$  を  $A_k$  倍した点  $A_v = A_k \times G$  を求め、 $R_a$ 、 $R_b$ 、 $A_v$  (X座標と Y座標) に対する電子署名  $A.Sig$  を生成し、A の公開鍵証明書とともに B に返送する。ここで、 $R_a$  および  $R_b$  はそれぞれ 64 ビット、 $A_v$  の X座標と Y座標がそれぞれ 160 ビットであるので、合計 448 ビットに対する電子署名を生成する。電子署名の生成方法は図 1 1 で説明したので、その詳細は省略する。また、公開鍵証明書も図 1 4 で説明したので、その詳細は省略する。

A の公開鍵証明書、 $R_a$ 、 $R_b$ 、 $A_v$ 、電子署名  $A.Sig$  を受信した B は、A が送信してきた  $R_b$  が、B が生成したものと一致するか検証する。その結果、一致していた場合には、A の公開鍵証明書内の電子署名を認証局の公開鍵で検証し、A の公開鍵を取り出す。公開鍵証明書の検証については、図 1 4 を用いて説明したので、その詳細は省略する。そして、取り出した A の公開鍵を用い電子署名  $A.Sig$  を検証する。電子署名の検証方法は図 1 2 で説明したので、その詳細は省略する。電子署名の検証に成功した後、B は A を正当なものとして認証する。

次に、Bは、標数 $p$ より小さい乱数 $B_k$ を生成する。そして、ベースポイント $G$ を $B_k$ 倍した点 $B_v = B_k \times G$ を求め、 $R_b$ 、 $R_a$ 、 $B_v$ （X座標とY座標）に対する電子署名 $B.Sig$ を生成し、Bの公開鍵証明書とともにAに返送する。

Bの公開鍵証明書、 $R_b$ 、 $R_a$ 、 $A_v$ 、電子署名 $B.Sig$ を受信したAは、Bが送信してきた $R_a$ が、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名 $B.Sig$ を検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

両者が認証に成功した場合には、Bは $B_k \times A_v$ （ $B_k$ は乱数だが、 $A_v$ は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、Aは $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

### （3－7）楕円曲線暗号を用いた暗号化処理

次に、楕円曲線暗号を用いた暗号化について、図16を用いて説明する。ステップS21において、 $M_x$ 、 $M_y$ をメッセージ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $G$ および $K_s \times G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS22で乱数 $u$ を $0 < u < r$ になるように生成し、ステップS23で公開鍵 $K_s \times G$ を $u$ 倍した座標 $V$ を計算する。なお、楕円曲線上のスカラー倍は図11のステップS4で説明したので、詳細は省略する。ステップS24で、 $V$ のX座標を $M_x$

倍して  $p$  で剰余を求め  $X_0$  とし、ステップ S 2 5 で  $V$  の  $Y$  座標を  $M_y$  倍して  $p$  で剰余を求め  $Y_0$  とする。なお、メッセージの長さが  $p$  のビット数より少ない場合、 $M_y$  は乱数を使い、復号化部では  $M_y$  を破棄するようにする。ステップ S 2 6 において、 $u \times G$  を計算し、ステップ S 2 7 で暗号文  $u \times G$ 、 $(X_0, Y_0)$  を得る。

### (3-8) 楕円曲線暗号を用いた復号化处理

次に、楕円曲線暗号を用いた復号化について、図 1 7 を用いて説明する。ステップ S 3 1 において、 $u \times G$ 、 $(X_0, Y_0)$  を暗号文データ、 $p$  を標数、 $a$ 、 $b$  を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$  を楕円曲線上のベースポイント、 $r$  を  $G$  の位数、 $K_s$  を秘密鍵（ $0 < K_s < r$ ）とする。ステップ S 3 2 において、暗号データ  $u \times G$  を秘密鍵  $K_s$  倍し、座標  $V(X_v, Y_v)$  を求める。ステップ S 3 3 では、暗号データの内、 $(X_0, Y_0)$  の  $X$  座標を取り出し、 $X_1 = X_0 / X_v \bmod p$  を計算し、ステップ S 3 4 においては、 $Y$  座標を取り出し、 $Y_1 = Y_0 / Y_v \bmod p$  を計算する。そして、ステップ S 3 5 で  $X_1$  を  $M_x$  とし、 $Y_1$  を  $M_y$  としてメッセージを取り出す。この時、 $M_y$  をメッセージにしていなかった場合、 $Y_1$  は破棄する。

このように、秘密鍵を  $K_s$ 、公開鍵を  $G$ 、 $K_s \times G$  とすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

また、公開鍵暗号の他の例としては RSA 暗号が知られているが、詳しい説明は省略する（PKCS #1 Version 2 に詳細が記述されている）。

### (3-9) 乱数生成処理

次に、乱数の生成方法について説明する。乱数の生成方法としては、熱雑音を増幅し、その A/D 出力から生成する真性乱数生成法や、M 系列等の線形回路を複数組み合わせ生成する疑似乱数生成法等が知られている。また、DES 等の共通鍵暗号を用いて生成する方法も知られている。本例では、DES を用いた疑似乱数生成方法について説明する（ANSI X9.17 ベース）。

まず、時間等のデータから得られた 64 ビット（これ以下のビット数の場合、

上位ビットを0とする)の値をD、Triple-DESに使われる鍵情報をK<sub>r</sub>、乱数発生用の種(Seed)をSとする。このとき、乱数Rは以下のように計算される。

$$I = \text{Triple-DES}(K_r, D) \cdots \cdots (2-1)$$

$$R = \text{Triple-DES}(K_r, S \wedge I) \cdots \cdots (2-2)$$

$$S = \text{Triple-DES}(K_r, R \wedge I) \cdots \cdots (2-3) \quad \cdots \cdots (2)$$

ここで、Triple-DES()は、第1引数を暗号鍵情報として、第2引数の値をTriple-DESで暗号化する関数とし、演算 $\wedge$ は64ビット単位の排他的論理和、最終的にでてきた値Sは、新規のSeed(種)として更新されていくものとする。

以下、連続して乱数を生成する場合には、(2-2)式、(2-3)式を繰り返すものとする。

以上、本発明のデータ処理装置において適用可能な暗号処理に関する各種処理態様について説明した。次に、本発明のデータ処理装置において実行される具体的な処理について、詳細に説明する。

#### (4) 記録再生器の格納データ構成

図18は、図3で示す記録再生器300での記録再生器暗号処理部302に構成された内部メモリ307のデータ保持内容を説明する図である。

図18に示すように、内部メモリ307には、以下の鍵、データが格納されている。

**MKake** : 記録再生器300と記録デバイス400(図3参照)との間で実行される相互認証処理に必要な認証鍵(Authentication and Key Exchange Key(以下、Kakeとする))を生成するための記録デバイス認証鍵用マスター鍵。

**IVake** : 記録デバイス認証鍵用初期値。

MKdis : 配送鍵Kdisを生成するための配送鍵用マスター鍵。

IVdis : 配送鍵生成用初期値。

Kicva : チェック値ICVaを生成するための鍵であるチェック値A生成鍵。

Kicvb : チェック値ICVbを生成するための鍵であるチェック値B生成鍵。

Kicvc : 各コンテンツブロックのチェック値ICVi ( $i = 1 \sim N$ ) を生成するための鍵であるコンテンツチェック値生成鍵。

Kicvt : 総チェック値ICVtを生成するための鍵である総チェック値生成鍵。

Ksys : 配信システムに共通の署名またはICVをつけるために使用するシステム署名鍵。

Kdev : 記録再生器毎に異なり、記録再生器が署名またはICVをつけるために使用する記録再生器固有の記録再生器署名鍵。

IVmem : 初期値、相互認証処理等の際の暗号処理に用いられる初期値。記録デバイスと共通。

これらの鍵、データが記録再生器暗号処理部302に構成された内部メモリ307に格納されている。

#### (5) 記録デバイスの格納データ構成

図19は、記録デバイス上でのデータ保持状況を示す図である。図19において、内部メモリ405は、複数のブロック（本例ではNブロック）に分割されており、それぞれのブロック中に、以下の鍵、データが格納されている。

IDmem : 記録デバイス識別情報、記録デバイス固有の識別情報。

Kake : 認証鍵、記録再生器300との相互認証時に用いる認証鍵。

IVmem : 初期値、相互認証処理等の際の暗号処理に用いられる初期値。

Kstr : 保存鍵、ブロック情報鍵他のコンテンツデータの暗号鍵。

Kr : 乱数生成鍵、

S : 種

これらのデータを個別のブロックに各々保持している。外部メモリ 402 は複数（本例では M 個）のコンテンツデータを保持しており、それぞれ図 4 で説明したデータを、例えば図 26、または図 27 のように保持している。図 26、図 27 の構成の差異については後段で説明する。

#### （6）記録再生器、記録デバイス間における相互認証処理

##### （6-1）相互認証処理の概要

図 20 は、記録再生器 300 と記録デバイス 400 との認証手順を示す流れ図である。ステップ S 41 において、利用者が記録デバイス 400 を記録再生器 300 に挿入する。ただし非接触で通信できる記録デバイスを使用する場合には、挿入する必要はない。

記録再生器 300 に記録デバイス 400 をセットすると、図 3 に示す記録再生器 300 内の記録デバイス検知手段（図示せず）が、制御部 301 に記録デバイス 400 の装着を通知する。次に、ステップ S 42 において、記録再生器 300 の制御部 301 は、記録デバイスコントローラ 303 を介して記録デバイス 400 に初期化命令を送信する。これを受信した記録デバイス 400 は、記録デバイス暗号処理部 401 の制御部 403 において、通信部 404 を介して命令を受信し、認証完了フラグがセットされていればクリアする。すなわち未認証状態に設定する。

次に、ステップ S 43 において、記録再生器 300 の制御部 301 は、記録再生器暗号処理部 302 に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器 300 に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス 400 との認証処理、およびデータ送受信が可能となる。

初期化命令を受信した記録再生器 300 の記録再生器暗号処理部 302 は、記録再生器暗号処理部 302 の制御部 306 において、記録デバイス挿入口番号に対応する認証完了フラグがセットされていればクリアする。すなわち未認証状態

に設定する。

次に、ステップS 4 4において、記録再生器3 0 0の制御部3 0 1は、記録デバイス4 0 0の記録デバイス暗号処理部4 0 1が使う鍵ブロック番号を指定する。なお、鍵ブロック番号の詳細に関しては後述する。ステップS 4 5において、記録再生器3 0 0の制御部3 0 1は、記録デバイス4 0 0の内部メモリ4 0 5の指定された鍵ブロックに格納された記録デバイス識別情報IDmemを読み出す。ステップS 4 6において、記録再生器3 0 0の制御部3 0 1は、記録再生器暗号処理部3 0 2に記録デバイス識別情報IDmemを送信し、記録デバイス識別情報IDmemに基づく認証鍵Kakeを生成させる。認証鍵Kakeの生成方法としては、例えば次のように生成する。

$$Kake = DES (MKake, IDmem \wedge IVake) \quad \dots\dots (3)$$

ここで、MKakeは、記録再生器3 0 0と記録デバイス4 0 0（図3参照）との間で実行される相互認証処理に必要な認証鍵Kakeを生成するための記録デバイス認証鍵用マスター鍵であり、これは、前述したように記録再生器3 0 0の内部メモリ3 0 7に格納されている鍵である。またIDmemは、記録デバイス4 0 0に固有の記録デバイス識別情報である。さらにIVakeは、記録デバイス認証鍵用初期値である。また、上記式において、DES（）は、第1引数を暗号鍵として、第2引数の値をDESで暗号化する関数であり、演算 $\wedge$ は64ビット単位の排他的論理和を示す。

例えば図7、図8に示すDES構成を適用する場合には、図7、8に示されるメッセージMを記録デバイス識別情報：IDmemとし、鍵K1をデバイス認証鍵用マスター鍵：MKakeとし、初期値IVを：IVakeとして得られる出力が認証鍵Kakeとなる。

次に、ステップS 4 7で相互認証およびセッション鍵Ksesの生成処理を行う。相互認証は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8と記録デ

バイス暗号処理部 401 の暗号／復号化部 406 の間で行われ、その仲介を記録再生器 300 の制御部 301 が行っている。

相互認証処理は、例えば前述の図 13 で説明した処理にしたがって実行することができる。図 13 に示す構成において、A、B がそれぞれ記録再生器 300 と記録デバイス 400 に対応する。まず、記録再生器 300 の記録再生器暗号処理部 302 が乱数  $R_b$  を生成し、乱数  $R_b$  および自己の ID である記録再生器識別情報  $ID_{dev}$  を記録デバイス 400 の記録デバイス暗号処理部 401 に送信する。なお、記録再生器識別情報  $ID_{dev}$  は、記録再生器 300 内に構成された記憶部に記憶された再生器固有の識別子である。記録再生器暗号処理部 302 の内部メモリ中に記録再生器識別情報  $ID_{dev}$  を記録する構成としてもよい。

乱数  $R_b$  および記録再生器識別情報  $ID_{dev}$  を受信した記録デバイス 400 の記録デバイス暗号処理部 401 は、新たに 64 ビットの乱数  $R_a$  を生成し、 $R_a$ 、 $R_b$ 、と記録再生器識別情報  $ID_{dev}$  の順に、DES の CBC モードで認証鍵  $K_{ake}$  を用いてデータを暗号化し、記録再生器 300 の記録再生器暗号処理部 302 に返送する。例えば、図 7 に示す DES の CBC モード処理構成によれば、 $R_a$  が  $M_1$ 、 $R_b$  が  $M_2$ 、 $ID_{dev}$  が  $M_3$  に相当し、初期値： $IV = IV_{mem}$  としたときの出力  $E_1$ 、 $E_2$ 、 $E_3$  が暗号文となる。

暗号文  $E_1$ 、 $E_2$ 、 $E_3$  を受信した記録再生器 300 の記録再生器暗号処理部 302 は、受信データを認証鍵  $K_{ake}$  で復号化する。受信データの復号化方法は、まず、暗号文  $E_1$  を認証鍵  $K_{ake}$  で復号化し、その結果と  $IV_{mem}$  とを排他的論理和し、乱数  $R_a$  を得る。次に、暗号文  $E_2$  を認証鍵  $K_{ake}$  で復号化し、その結果と  $E_1$  を排他的論理和し、 $R_b$  を得る。最後に、暗号文  $E_3$  を認証鍵  $K_{ake}$  で復号化し、その結果と  $E_2$  を排他的論理和し、記録再生器識別情報  $ID_{dev}$  を得る。こうして得られた  $R_a$ 、 $R_b$ 、記録再生器識別情報  $ID_{dev}$  の内、 $R_b$  および記録再生器識別情報  $ID_{dev}$  が、記録再生器 300 が送信したものと一致するか検証する。この検証に通った場合、記録再生器 300 の記録再生器暗号処理部 302 は記録デバイス 400 を正当なものとして認証する。

次に、記録再生器 300 の記録再生器暗号処理部 302 は、認証後に使用するセッション鍵 (Session Key (以下、Kses とする)) を生成する (生成方法は、乱数を用いる)。そして、Rb、Ra、Kses の順に、DES の CBC モードで鍵 Kake、初期値 IVmem を用いて暗号化し、記録デバイス 400 の記録デバイス暗号処理部 401 に返送する。

これを受信した記録デバイス 400 の記録デバイス暗号処理部 401 は、受信データを鍵 Kake で復号化する。受信データの復号化方法は、記録再生器 300 の記録再生器暗号処理部 302 における復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた Rb、Ra、Kses の内、Rb および Ra が、記録デバイス 400 が送信したものと一致するか検証する。この検証に通った場合、記録デバイス 400 の記録デバイス暗号処理部 401 は記録再生器 300 を正当なものとして認証する。互いに相手を認証した後には、セッション鍵 Kses は、認証後の秘密通信のための共通鍵として利用される。

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

相互認証に成功した場合には、ステップ S48 からステップ S49 に進み、セッション鍵 Kses を記録再生器 300 の記録再生器暗号処理部 302 で保持するとともに、相互認証が終了したことを示す認証完了フラグをセットする。また、相互認証に失敗した場合には、ステップ S50 に進み、認証処理過程で生成されたセッション鍵 Kses を破棄するとともに、認証完了フラグをクリアする。なお、すでにクリアされている場合には必ずしもクリア処理は必要ではない。

なお、記録デバイス 400 が記録デバイス挿入口から取り除かれた場合には、記録再生器 300 内の記録デバイス検知手段が、記録再生器 300 の制御部 301 に記録デバイス 400 が取り除かれたことを通知し、これを受けた記録再生器 300 の制御部 301 は、記録再生器 300 の記録再生器暗号処理部 302 に対し記録デバイス挿入口番号に対応する認証完了フラグをクリアするように命令し、これを受けた記録再生器 300 の記録再生器暗号処理部 302 は、記録デバイ

ス挿入口番号に対応する認証完了フラグをクリアする。

なお、ここでは相互認証処理を図 13 に示す手続きにしたがって実行する例について説明したが、上述した認証処理例に限らず、例えば先に説明した図 15 の相互認証手続きに従った処理を実行してもよい。また、図 13 に示す手続きにおいて、図 13 の A を記録再生器 300 とし、B を記録デバイス 400 とし、B : 記録デバイス 400 が A : 記録再生器 300 に最初に送付する ID を記録デバイス中の鍵ブロック中の記録デバイス識別情報として相互認証処理を行なってもよい。本発明において実行される認証処理手続きは、様々な処理が適用可能であり、上述の認証処理に限定されるものではない。

#### (6-2) 相互認証時の鍵ブロックの切り替え

本発明のデータ処理装置における相互認証処理における 1 つの特徴は、記録デバイス 400 側に複数の鍵ブロック (ex. N 個の鍵ブロック) を構成して、記録再生器 300 が 1 つの鍵ブロックを指定 (図 20 の処理フローにおけるステップ S44) して認証処理を実行する点である。先に図 19 において説明したように、記録デバイス 400 の暗号処理部 401 に構成された内部メモリ 405 には複数の鍵ブロックが形成されており、それぞれが異なる鍵データ、ID 情報等各種データを格納している。図 20 で説明した記録再生器 300 と記録デバイス 400 間で実行される相互認証処理は、図 19 の記録デバイス 400 の複数の鍵ブロックの 1 つの鍵ブロックに対して実行される。

従来、記憶媒体とその再生機器間における相互認証処理を実行する構成では、相互認証に用いる鍵 : 認証鍵は共通なものが使用されるのが一般的であった。従って、例えば製品仕向け先 (国別) ごと、あるいは製品ごとに認証鍵を変更しようとする、記録再生器側と、記録デバイス側の認証処理に必要な鍵データを双方の機器において変更することが必要となる。従って例えば新たに発売された記録再生器に格納された認証処理に必要な鍵データは、先に販売された記録デバイスに格納された認証処理に必要な鍵データに対応せず、新たな記録再生器は、古いバージョンの記録デバイスへのアクセスができなくなってしまう

事態が発生する。逆に新しいバージョンの記録デバイスと古いバージョンの記録再生器との関係においても同様の事態が発生する。

本発明のデータ処理装置においては、図19に示すように予め記録デバイス400に複数の異なる鍵セットとしての鍵ブロックが格納されている。記録再生器は例えば製品仕向け先（国別）ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロック、すなわち指定鍵ブロックが設定される。この設定情報は、記録再生器のメモリ部、例えば、図3における内部メモリ307、あるいは、記録再生器300の有するその他の記憶素子内に格納され、認証処理時に図3の制御部301によってアクセスされ設定情報にしたがった鍵ブロック指定が行われる。

記録再生器300の内部メモリ307の記録デバイス認証鍵用マスター鍵MKakeは、それぞれの指定鍵ブロックの設定に従って設定された認証鍵用マスター鍵であり、指定鍵ブロックにのみ対応可能となっており、指定鍵ブロック以外の鍵ブロックとの相互認証は成立しない構成となっている。

図19から理解されるように、記録デバイス400の内部メモリ405には1～NのN個の鍵ブロックが設定され、各鍵ブロック毎に記録デバイス識別情報、認証鍵、初期値、保存鍵、乱数生成鍵、種が格納され、少なくとも認証用のかぎデータがブロック毎に異なるデータとして格納されている。

このように、記録デバイス400の鍵ブロックの鍵データ構成は、ブロック毎に異なっている。従って、例えば、ある記録再生機器Aが内部メモリに格納された記録デバイス認証鍵用マスター鍵MKakeを用いて認証処理を行ない得る鍵ブロックは鍵ブロックNo. 1であり、また別の仕様の記録再生器Bが認証可能な鍵ブロックは別の鍵ブロック、例えば鍵ブロックNo. 2のように設定することが可能となる。

後段でさらに詳細に説明するが、コンテンツを記録デバイス400の外部メモリ402に格納する際、各鍵ブロックに格納された保存鍵Kstrを用いて暗号化処理がなされ、格納されることになる。より、具体的には、コンテンツブロッ

クを暗号化するコンテンツ鍵を保存鍵で暗号化処理する。

図19に示すように保存鍵は、各ブロック毎に異なる鍵として構成されている。従って、異なる鍵ブロックを指定するように設定された2つの異なる設定の記録再生器間においては、ある1つの記録デバイスのメモリに格納されたコンテンツを両方で共通に利用することは防止される。すなわち、異なる設定のなされた記録再生器は、それぞれの設定に合致する記録デバイスに格納されたコンテンツのみが利用できる。

なお、各鍵ブロックについて共通化可能なデータは共通化することも可能であり、例えば認証用の鍵データ、保存鍵データのみを異なるように構成してもよい。

このような記録デバイスに複数の異なる鍵データからなる鍵ブロックを構成する具体例としては、例えば記録再生器300の機種別（据え置き型、携帯型等）で指定すべき鍵ブロック番号を異なるように設定したり、あるいは、アプリケーション毎に指定鍵ブロックを異なるように設定する例がある。さらに、例えば日本で販売する記録再生器については指定鍵ブロックをNo. 1とし、米国で販売する記録再生器は指定鍵ブロックをNo. 2とするように地域ごとに異なる鍵ブロック設定を行なう構成とすることも可能である。このような構成とすることで、それぞれの異なる販売地域で使用され、記録デバイスに異なる保存鍵で格納されたコンテンツは、たとえメモリカードのような記録デバイスが米国から日本、あるいは日本から米国へ転送されてきても、異なる鍵設定のなされた記録再生器で利用することは不可能であるので、メモリに格納したコンテンツの不正、無秩序な流通を防止できる。具体的には、異なる保存鍵K<sub>str</sub>で暗号化されているコンテンツ鍵K<sub>con</sub>が2国間で相互に利用可能となる状態を排除することができる。

さらに、図19に示す記録デバイス400の内部メモリ405の鍵ブロック1～Nまでの少なくとも1つの鍵ブロック、例えばNo. Nの鍵ブロックをいずれの記録再生器300においても共通に利用可能な鍵ブロックとして構成してもよ

い。

例えば、全ての機器に鍵ブロック No. N との認証可能な記録デバイス認証鍵用マスター鍵 MK a k e を格納することで、記録再生器 300 の機種別、アプリケーション毎、仕向け国毎等に関係なく流通可能なコンテンツとして扱うことができる。例えば、鍵ブロック No. N に格納された保存鍵でメモリカードに格納された暗号化コンテンツは、すべての機器において利用可能なコンテンツとなる。例えば、音楽データ等を共通に利用可能な鍵ブロックの保存鍵で暗号化してメモリカードに記憶し、このメモリカードを、やはり共通の記録デバイス認証鍵用マスター鍵 MK a k e を格納した例えば携帯型の音声再生機器等にセットすることで、メモリカードからのデータの復号再生処理を可能とすることができる。

本発明のデータ処理装置における複数の鍵ブロックを有する記録デバイスの利用例を図 21 に示す。記録再生器 2101 は日本向け製品の記録再生器であり、記録デバイスの鍵ブロックの No. 1, 4 との間での認証処理が成立するマスター鍵を持っている。記録再生器 2102 は US 向け製品の記録再生器であり、記録デバイスの鍵ブロックの No. 2, 4 との間での認証処理が成立するマスター鍵を持っている。記録再生器 2103 は EU 向け製品の記録再生器であり、記録デバイスの鍵ブロックの No. 3, 4 との間での認証処理が成立するマスター鍵を持っている。

例えば記録再生器 2101 は、記録デバイス A, 2104 の鍵ブロック 1 または鍵ブロック 4 との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器 2102 は、記録デバイス B, 2105 の鍵ブロック 2 または鍵ブロック 4 との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器 2103 は、記録デバイス C, 2106 の鍵ブロック 3 または鍵ブロック 4 との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。ここで、記録デバイス A, 2104 を記録再生器 2

102、または記録再生器2103に装着した場合、鍵ブロック1の保存鍵で暗号処理がなされたコンテンツは、記録再生器2102、記録再生器2103と鍵ブロック1との間での認証が成立しないので利用不可能となる。一方、鍵ブロック4の保存鍵で暗号処理がなされたコンテンツは、記録再生器2102、記録再生器2103と鍵ブロック4との間での認証が成立するので利用可能となる。

上述のように、本発明のデータ処理装置においては、記録デバイスに複数の異なる鍵セットからなる鍵ブロックを構成し、一方、記録再生機器には、特定の鍵ブロックに対する認証可能なマスター鍵を格納する構成としたので、様々な利用態様に応じたコンテンツの利用制限を設定することが可能となる。

なお、1つの記録再生機器において指定可能な鍵ブロックを複数、例えば1～kとし、他の記録再生器において指定可能な鍵ブロックをp～qのように複数とすることも可能であり、また、共通に利用可能な鍵ブロックを複数設ける構成としてもよい。

#### (7) 記録再生器から記録デバイスへのダウンロード処理

次に、本発明のデータ処理装置において、記録再生器300から記録デバイス400の外部メモリにコンテンツをダウンロードする処理について説明する。

図22は、記録再生器300から記録デバイス400へコンテンツをダウンロードする手順を説明する流れ図である。なお、図22においては、既に記録再生器300と記録デバイス400との間で上述した相互認証処理が完了しているものとする。

ステップS51において、記録再生器300の制御部301は、読み取り部304を使ってコンテンツを格納したメディア500から所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信する。そして、記録再生器300の制御部301は、データの内ヘッダ(Header)部分(図4参照)を記録再生器300の記録再生器暗号処理部302に送信する。

次に、ステップS52において、ステップS51でヘッダ(Header)を

受信した記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にチェック値 A を計算させる。チェック値 A は、図 23 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 A 生成鍵  $K_{icva}$  を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明した ICV 計算方法に従って計算される。なお、初期値は、 $IV = 0$  としても、記録再生器暗号処理部 302 の内部メモリ 307 にチェック値 A 生成用初期値  $IV_a$  を保存しておき、それを使用してもよい。最後に、チェック値 A とヘッダ (Header) 内に格納されたチェック値:  $ICV_a$  を比較し、一致していた場合にはステップ S53 へ進む。

先に図 4 において説明したようにチェック値 A、 $ICV_a$  は、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 A 生成鍵  $K_{icva}$  を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明した ICV 計算方法に従って計算されるチェック値 A が、ヘッダ (Header) 内に格納されたチェック値:  $ICV_a$  と一致した場合には、識別情報、取扱方針の改竄はないと判断される。

次に、ステップ S53 において、記録再生器暗号処理部 302 の制御部 306 は、配送鍵  $K_{dis}$  の生成を記録再生器暗号処理部 302 の暗号／復号化部 308 に行わせる。配送鍵  $K_{dis}$  の生成方法としては、例えば次のように生成する。

$$K_{dis} = DES (MK_{dis}, ContentID \oplus IV_{dis}) \dots (4)$$

ここで、 $MK_{dis}$  は、配送鍵  $K_{dis}$  を生成するための配送鍵用マスター鍵であり、これは、前述したように記録再生器 300 の内部メモリに格納されている鍵である。また Content ID はコンテンツデータのヘッダ部の識別情

報であり、さらに  $IVdis$  は、配送鍵用初期値である。また、上記式において、 $DES()$  は、第1引数を暗号鍵として、第2引数の値を暗号化する関数であり、演算 $\wedge$ は64ビット単位の排他的論理和を示す。

ステップS54において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308を使って、ステップS53で生成した配送鍵 $Kdis$ を用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵 $Kbit$ とコンテンツ鍵 $Kcon$ （図4参照）の復号化処理を行う。図4に示されるようにこれらブロック情報鍵 $Kbit$ とコンテンツ鍵 $Kcon$ は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、配送鍵 $Kdis$ によって予め暗号化処理が施されている。

さらに、ステップS55において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308を使って、ステップS54で復号化したブロック情報鍵 $Kbit$ でブロック情報（BIT）を復号化する。図4に示されるようにブロック情報（BIT）は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、ブロック情報鍵 $Kbit$ によって予め暗号化処理が施されている。

さらに、ステップS56において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵 $Kbit$ 、コンテンツ鍵 $Kcon$ およびブロック情報（BIT）を8バイト単位に分割し、それら全てを排他的論理和する（加算、減算等、いずれの演算でもよい）。次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にチェック値 $B(ICVb)$ を計算させる。チェック値 $B$ は、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値 $B$ 生成鍵 $Kicvb$ を鍵とし、先ほど計算した排他的論理和値をDESで暗号化して生成する。最後に、チェック値 $B$ とHeader内の $ICVb$ を比較し、一致していた場合にはステップS57へ進む。

先に図4において説明したように、チェック値B、ICVbは、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報(BIT)の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:ICVbと一致した場合には、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄はないと判断される。

ステップS57において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したヘッダ(Header)内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7で説明したICV計算方法に従って計算する。なお、初期値IV=0としても、記録再生器暗号処理部302の内部メモリ307に総チェック値生成用初期値IVtを保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。

この中間チェック値は、チェック値A、チェック値B、全てのコンテンツチェック値をメッセージとして生成されるものであり、これらの各チェック値の検証対象となっているデータについての検証を中間チェック値の照合処理によって行なってもよい。しかし、本実施例においては、システム全体の共有データとしての非改竄性検証処理と、ダウンロード処理後に各記録再生機器300のみが占有する占有データとして識別するための検証処理を区別して実行可能とするために、中間チェック値からさらに複数の異なるチェック値、すなわち総チェック値ICVtと、記録再生器固有チェック値ICVdevとを別々に、中間チェック値

に基づいて生成可能としている。これらのチェック値については後段で説明する。

記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に総チェック値  $ICV_t$  の計算をさせる。総チェック値  $ICV_t$  は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵  $K_{sys}$  を鍵とし、中間チェック値を DES で暗号化して生成する。最後に、生成した総チェック値  $ICV_t$  とステップ S51 で保存しておいた Header 内の  $ICV_t$  を比較し、一致していた場合には、ステップ S58 へ進む。システム署名鍵  $K_{sys}$  は、複数の記録再生器、すなわちある一定のデータの記録再生処理を実行するシステム集合全体において共通する署名鍵である。

先に図 4 において説明したように、総チェック値  $ICV_t$  は、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ (Header) 内に格納されたチェック値： $ICV_t$  と一致した場合には、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

次に、ステップ S58 において、記録再生器 300 の制御部 301 は、ブロック情報 (BIT) 内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録再生器 300 の読み取り部 304 を使ってメディア 500 から読み出すか、記録再生器 300 の通信部 305 を使って通信手段 600 から受信し、記録再生器 300 の記録再生器暗号処理部 302 へ送信する。これを受信した記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の

暗号／復号化部 308 にコンテンツ中間値を計算させる。

コンテンツ中間値は、ステップ S54 で復号化したコンテンツ鍵  $K_{con}$  で、入力されたコンテンツブロックを DES の CBC モードで復号化し、その結果を 8 バイトごとに区切り、全て排他的論理和（加算、減算等、いずれの演算でもよい）して生成する。

次に、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているコンテンツチェック値生成鍵  $K_{icvc}$  を鍵とし、コンテンツ中間値を DES で暗号化して生成する。そして、記録再生器暗号処理部 302 の制御部 306 は、当該コンテンツチェック値と、ステップ S51 で記録再生器 300 の制御部 301 から受信したコンテンツブロック内の ICV を比較し、その結果を記録再生器 300 の制御部 301 に渡す。これを受信した記録再生器 300 の制御部 301 は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器 300 の記録再生器暗号処理部 302 に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、Header 生成側と合わせておけば、 $IV=0$  としても、記録再生器暗号処理部 302 の内部メモリ 307 にコンテンツチェック値生成用初期値  $IV_c$  を保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器 300 の記録再生器暗号処理部 302 に保持しておく。さらにまた、記録再生器 300 の記録再生器暗号処理部 302 は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを 2 回以上検証させられたりした場合には、認証に失敗したものとする。そして、全ての検証が成功した場合には、ステップ S59 へ進む。

次に、ステップ S59 において、記録再生器 300 の記録再生器暗号処理部 302 は、ステップ S54 で復号化しておいたブロック情報鍵  $K_{bit}$  とコンテンツ鍵  $K_{con}$  を、記録再生器暗号処理部 302 の暗号／復号化部 308 に、相互

認証の際に共有しておいたセッション鍵  $K_{ses}$  で暗号化させる。記録再生器 300 の制御部 301 は、セッション鍵  $K_{ses}$  で暗号化されたブロック情報鍵  $K_{bit}$  とコンテンツ鍵  $K_{con}$  を記録再生器 300 の記録再生器暗号処理部 302 から読み出し、これらのデータを記録再生器 300 の記録デバイスコントローラ 303 を介して記録デバイス 400 に送信する。

次に、ステップ S60 において、記録再生器 300 から送信されてきたブロック情報鍵  $K_{bit}$  とコンテンツ鍵  $K_{con}$  を受信した記録デバイス 400 は、受信したデータを記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵  $K_{ses}$  で復号化させ、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵  $K_{str}$  で再暗号化させる。最後に、記録再生器 300 の制御部 301 は、記録再生器 300 の記録デバイスコントローラ 303 を介し、記録デバイス 400 から保存鍵  $K_{str}$  で再暗号化されたブロック情報鍵  $K_{bit}$  とコンテンツ鍵  $K_{con}$  を読み出す。そして、これらの鍵を、配送鍵  $K_{dis}$  で暗号化されたブロック情報鍵  $K_{bit}$  とコンテンツ鍵  $K_{con}$  に置き換える。

ステップ S61 において、記録再生器 300 の制御部 301 は、データのヘッダ部の取扱方針 (Usage Policy) から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器 300 のみで利用できる (この場合、利用制限情報が 1 に設定) か、別の同様な記録再生器 300 でも利用できる (この場合、利用制限情報が 0 に設定) か判定する。判定の結果、利用制限情報が 1 であった場合には、ステップ S62 に進む。

ステップ S62 において、記録再生器 300 の制御部 301 は、記録再生器固有のチェック値を記録再生器 300 の記録再生器暗号処理部 302 に計算させる。記録再生器固有のチェック値は、図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器署名鍵  $K_{dev}$  を鍵とし、ステップ S58 で保持しておいた中間チェック値を DES で暗号化して生成する。計算された記録再生器固有のチェック値  $ICV_{dev}$  は、総チェック値  $ICV$

t の代わりに上書きされる。

先に説明したように、システム署名鍵  $K_{sys}$  は、配信システムに共通の署名または  $ICV$  をつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵  $K_{dev}$  は、記録再生器毎に異なり、記録再生器が署名または  $ICV$  をつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵  $K_{sys}$  によって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値  $ICV_t$  が一致することになるので、共通に利用可能となるが、記録再生器署名鍵  $K_{dev}$  を用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵  $K_{dev}$  を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値  $ICV_{dev}$  が不一致となり、エラーとなるので再生できないことになる。

従って、本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

ステップ  $S63$  において、記録再生器  $300$  の制御部  $301$  は、コンテンツを記録デバイス  $400$  の外部メモリ  $402$  に保存する。

図  $26$  は、利用制限情報が  $0$  の場合における記録デバイス内のコンテンツ状況を示す図である。図  $27$  は、利用制限情報が  $1$  の場合における記録デバイス内のコンテンツ状況を示す図である。図  $26$  が図  $4$  と異なる点は、コンテンツブロック情報鍵  $K_{bit}$  とコンテンツ鍵  $K_{con}$  が配送鍵  $K_{dis}$  で暗号化されているか、保存鍵  $K_{str}$  で暗号化されているかだけである。また、図  $27$  が図  $26$  と異なる点は、中間チェック値から計算されるチェック値が、図  $26$  ではシステム署名鍵  $K_{sys}$  で暗号化されているのに対し、図  $27$  では記録再生器固有の記録再生器署名鍵  $K_{dev}$  で暗号化されていることである。

なお、図  $22$  の処理フローにおいて、ステップ  $S52$  でチェック値  $A$  の検証に

失敗した場合、ステップS 5 6でチェック値Bの検証に失敗した場合、ステップS 5 7で総チェック値ICV<sub>t</sub>の検証に失敗した場合、ステップS 5 8で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合には、ステップS 6 4に進み、所定のエラー表示を行う。

また、ステップS 6 1で利用制限情報が0であった場合には、ステップS 6 2をスキップしてステップS 6 3へ進む。

#### (8) 記録デバイス格納情報の記録再生器での再生処理

次に記録デバイス400の外部メモリ402に格納されたコンテンツ情報の記録再生器300での再生処理について説明する。

図28は、記録再生器300が記録デバイス400からコンテンツを読み出し、コンテンツを利用する手順を説明する流れ図である。なお、図28においても、既に記録再生器300と記録デバイス400との間で相互認証が完了しているものとする。

ステップS 7 1において、記録再生器300の制御部301は、記録デバイスコントローラ303を使って記録デバイス400の外部メモリ402からコンテンツを読み出す。そして、記録再生器300の制御部301は、データの内のヘッダ(Header)部分を記録再生器300の記録再生器暗号処理部302に送信する。ステップS 7 2は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS 5 2と同様の処理であり、ヘッダ(Header)を受信した記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる処理である。チェック値Aは、先に説明した図23に示すように記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K<sub>icva</sub>を鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したと同様のICV計算方法に従って計算される。

先に説明したようにチェック値A、ICV<sub>a</sub>は、識別情報、取扱方針の改竄を

検証するためのチェック値である。記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 A 生成鍵 K i c v a を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明した I C V 計算方法に従って計算されるチェック値 A が、ヘッダ (Header) 内に格納されたチェック値: I C V a と一致した場合には、記録デバイス 400 に格納された識別情報、取扱方針の改竄はないと判断される。

次に、ステップ S 73 において、記録再生器 300 の制御部 301 は、読み出したヘッダ (Header) 部分からブロック情報鍵 K b i t とコンテンツ鍵 K c o n を取り出し、記録再生器 300 の記録デバイスコントローラ 303 を介して記録デバイス 400 に送信する。記録再生器 300 から送信されてきたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を受信した記録デバイス 400 は、受信したデータを記録デバイス暗号処理部 401 の暗号／復号化部 406 に、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵 K s t r で復号化処理させ、相互認証の際に共有しておいたセッション鍵 K s e s で再暗号化させる。そして、記録再生器 300 の制御部 301 は、記録再生器 300 の記録デバイスコントローラ 303 を介し、記録デバイス 400 からセッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を読み出す。

次に、ステップ S 74 において、記録再生器 300 の制御部 301 は、受信したセッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を記録再生器 300 の記録再生器暗号処理部 302 に送信する。

セッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を受信した記録再生器 300 の記録再生器暗号処理部 302 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に、セッション鍵 K s e s で暗号化されたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を、相互認証の際に共有しておいたセッション鍵 K s e s で復号化させる。そして、復号化したプロ

ック情報鍵K b i tで、ステップS 7 1で受信しておいたブロック情報を復号化させる。

なお、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、復号化したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tを、ステップS 7 1で受信しておいたブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tに置き換えて保持しておく。また、記録再生器3 0 0の制御部3 0 1は、復号化されたブロック情報B I Tを記録再生器3 0 0の記録再生器暗号処理部3 0 2から読み出しておく。

ステップS 7 5は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS 5 6と同様の処理である。記録再生器暗号処理部3 0 2の制御部3 0 6が、記録デバイス4 0 0から読み出したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報(B I T)を8バイト単位に分割し、それら全てを排他的論理和する。次に、記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にチェック値B ( I C V b)を計算させる。チェック値Bは、先に説明した図2 4に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、先ほど計算した排他的論理和値をD E Sで暗号化して生成する。最後に、チェック値BとH e a d e r内のI C V bを比較し、一致していた場合にはステップS 7 6へ進む。

先に説明したように、チェック値B, I C V bは、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、記録デバイス4 0 0から読み出したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報(B I T)を8バイト単位に分割し排他的論理和して得られる値をD E Sで暗号化して生成したチェック値Bが、記録デバイス4 0 0から読み出したデータ中のヘッダ(H e a d e r)内に格納されたチェック値: I C V bと一致した場合には、記録デバイス4 0 0

に格納されたデータのブロック情報鍵  $K_{bit}$ 、コンテンツ鍵  $K_{con}$ 、ブロック情報の改竄はないと判断される。

ステップ S 7 6 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に中間チェック値の計算をさせる。中間チェック値は、先に説明した図 2 5 に示すように記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されている総チェック値生成鍵  $K_{icvt}$  を鍵とし、検証したヘッダ (Header) 内のチェック値 A、チェック値 B、保持しておいた全てのコンテンツチェック値をメッセージとして図 7 他で説明した ICV 計算方法に従って計算する。なお、初期値は  $IV = 0$  としても、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に総チェック値生成用初期値に  $IV_t$  を保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に保持しておく。

次に、ステップ S 7 7 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録デバイス 4 0 0 の外部メモリ 4 0 2 から読み出したデータのヘッダ部に含まれる取扱方針 (Usage Policy) から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器 3 0 0 のみで利用できる (利用制限情報が 1) か、別の同様な記録再生器 3 0 0 でも利用できる (利用制限情報が 0) か判定する。判定の結果、利用制限情報が 1、すなわちダウンロードしたコンテンツが当該記録再生器 3 0 0 のみで利用できる利用制限が設定されている場合には、ステップ S 8 0 に進み、利用制限情報が 0、すなわち別の同様な記録再生器 3 0 0 でも利用できる設定であった場合には、ステップ S 7 8 に進む。なお、ステップ S 7 7 の処理は、暗号処理部 3 0 2 が行なってもよい。

ステップ S 7 8 においては、(7) 記録再生器から記録デバイスへのダウンロード処理において説明したステップ S 5 8 と同様の総チェック値  $ICV_t$  の計算が実行される。すなわち、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に総チェック値  $ICV_t$  の計算をさせる。総チェック値  $ICV_t$  は、先に説明した図 2 5 に示すように記録再生

器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵  $K_{sys}$  を鍵とし、中間チェック値を DES で暗号化して生成する。

次に、ステップ S79 に進み、ステップ S78 において生成した総チェック値  $ICV_t$  とステップ S71 で保存しておいたヘッダ (Header) 内の  $ICV_t$  を比較し、一致していた場合には、ステップ S82 へ進む。

先に説明したように、総チェック値  $ICV_t$  は、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ (Header) 内に格納されたチェック値： $ICV_t$  と一致した場合には、記録デバイス 400 に格納されたデータにおいて、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

ステップ S77 での判定において、ダウンロードしたコンテンツが当該記録再生器 300 のみで利用できる設定であった場合、すなわち設定情報が 1 であった場合は、ステップ S80 に進む。

ステップ S80 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に、記録再生器固有のチェック値  $ICV_{dev}$  の計算をさせる。記録再生器固有のチェック値  $ICV_{dev}$  は、先に説明した図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器固有の記録再生器署名鍵  $K_{dev}$  を鍵とし、中間チェック値を DES で暗号化して生成する。ステップ S81 において、ステップ S80 で計算した記録再生器固有のチェック値  $ICV_{dev}$  とステップ S71 で保存しておいた Header 内の  $ICV_{dev}$  を比較し、一致していた場合には、ステップ S82 へ進む。

このように、システム署名鍵  $K_{sys}$  によって署名されたデータは、同じシステム署名鍵を有するシステム (記録再生器) によってチェックが成功、すなわち総チェック値  $ICV_t$  が一致することになるので共通に利用可能となり、記録再生器署名鍵  $K_{dev}$  を用いて署名された場合には、記録再生器署名鍵はその記録

再生器に固有の鍵であるので、記録再生器署名鍵 $K_{dev}$ を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値 $ICV_{dev}$ が不一致となり、エラーとなるので再生できないことになる。従って、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

ステップS82において、記録再生器300の制御部301は、ステップS74で読み出しておいたブロック情報BIT内のコンテンツブロック情報を取り出し、コンテンツブロックが暗号化対象になっているかいないか調べる。暗号化対象になっていた場合には、該当するコンテンツブロックを、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400の外部メモリ402から読み出し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツを復号化させるとともに、コンテンツブロックが検証対象になっている場合には次のステップS83においてコンテンツチェック値を検証させる。

ステップS83は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS58と同様の処理である。記録再生器300の制御部301は、ブロック情報(BIT)内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないかをコンテンツチェック値の格納状況から判定し、コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録デバイス400の外部メモリ402から受信し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツ中間値を計算させる。

コンテンツ中間値は、ステップS74で復号化したコンテンツ鍵 $K_{con}$ で、

入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を8バイトに区切り全て排他的論理和して生成する。

次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部302の内部メモリ307に保存されているコンテンツチェック値生成鍵K<sub>icvc</sub>を鍵とし、コンテンツ中間値をDESで暗号化して生成する。そして、記録再生器暗号処理部302の制御部306は、当該コンテンツチェック値と、ステップS71で記録再生器300の制御部301から受信したコンテンツブロック内のICVを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、初期値はIV=0としても、記録再生器暗号処理部302の内部メモリ307にコンテンツチェック値生成用初期値IV<sub>c</sub>を保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器300の記録再生器暗号処理部302に保持しておく。さらにまた、記録再生器300の記録再生器暗号処理部302は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。

記録再生器300の制御部301は、当該コンテンツチェック値の比較結果(検証対象になっていない場合、比較結果は全て成功とする)を受信し、検証に成功していた場合には、記録再生器300の記録再生器暗号処理部302から復号化されたコンテンツを取り出す。そして、次の復号化対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に復号化させ、全てのコンテンツブロックを復号化するまで繰り返す。

なお、ステップS83において、記録再生器300の記録再生器暗号処理部3

02は、コンテンツチェック値の検証処理において不一致となった場合には、検証失敗としてその時点で処理を中止し、残るコンテンツの復号化は行わない。また、記録再生器300の記録再生器暗号処理部302は、復号化対象のコンテンツブロックの復号化順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上復号化させられたりした場合には、復号化に失敗したものとする。

なお、ステップS72でチェック値Aの検証に失敗した場合、ステップS75でチェック値Bの検証に失敗した場合、ステップS79で総チェック値ICV<sub>t</sub>の検証に失敗した場合、ステップS81で記録再生器固有のチェック値ICV<sub>dev</sub>の検証に失敗した場合には、ステップS83で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合、ステップS84に進み、所定のエラー表示を行う。

以上説明してきたように、コンテンツをダウンロードしたり、利用したりする際に、重要なデータやコンテンツを暗号化しておいて隠蔽化したり、改竄検証ができるだけでなく、ブロック情報BITを復号化するためのブロック情報鍵K<sub>bit</sub>、コンテンツを復号化するためのコンテンツ鍵K<sub>con</sub>が記録デバイス固有の保存鍵K<sub>str</sub>で保存されているため、単純に記録メディア上のデータを別の記録メディアに複製したとしても、コンテンツを正しく復号化することができなくすることができる。より具体的には、例えば図28のステップS74において、記録デバイス毎に異なる保存鍵K<sub>str</sub>で暗号化されたデータを復号化するため、別の記録デバイスではデータを正しく復号化できない構成を持つからである。

#### (9) 相互認証後の鍵交換処理

本発明のデータ処理装置における特徴の1つに、上述した記録再生器300と記録デバイス400との間で実行される相互認証処理の後においてのみ、記録デバイスの利用を可能とし、また、その利用態様を制限した点がある。

例えば、不正な複製等によってコンテンツを格納したメモ리카ード等の記録デ

バースを生成し、これを記録再生器にセットして利用されることを排除するために、記録再生器 300 と、記録デバイス 400 間での相互認証処理を実行し、かつ認証 OK となったことを条件として、コンテンツ（暗号化された）の記録再生器 300 および記録デバイス 400 間での転送を可能としている。

上記の制限的処理を実現するために、本発明のデータ処理装置においては、記録デバイス 400 の暗号処理部 401 での処理は、すべて、予め設定されたコマンド列に基づいて実行される構成となっている。すなわち、記録デバイスは、コマンド番号に基づくコマンドを順次レジスタから取り出して実行するコマンド処理構成を持つ。この記録デバイスでのコマンド処理構成を説明する図を図 29 に示す。

図 29 に示すように記録再生器暗号処理部 302 を有する記録再生器 300 と記録デバイス暗号処理部 401 を有する記録デバイス 400 間においては、記録再生器 300 の制御部 301 の制御のもとに記録デバイスコントローラ 303 から記録デバイス 400 の通信部（受信レジスタを含む）404 に対してコマンド番号（No.）が出力される。

記録デバイス 400 は、暗号処理部 401 内の制御部 403 にコマンド番号管理部 2201 を有する。コマンド番号管理部 2901 は、コマンドレジスタ 2902 を保持しており、記録再生器 300 から出力されるコマンド番号に対応するコマンド列を格納している。コマンド列は、図 29 の右に示すようにコマンド番号 0 から y まで順次、コマンド番号に対して実行コマンドが対応付けされている。コマンド番号管理部 2901 は、記録再生器 300 から出力されるコマンド番号を監視し、対応するコマンドをコマンドレジスタ 2902 から取り出して実行する。

コマンドレジスタ 2902 に格納されたコマンドシーケンスは、図 29 の右に示すように、認証処理シーケンスに関するコマンド列が先行するコマンド番号 0 ～ k に対応付けられている。さらに、認証処理シーケンスに関するコマンド列の後のコマンド番号 p ～ s に復号、鍵交換、暗号処理コマンドシーケンス 1、さら

に、後続するコマンド番号u～yに復号、鍵交換、暗号処理コマンドシーケンス2が対応付けされている。

先に図20の認証処理フローにおいて説明したように、記録デバイス400が記録再生器300に装着されると、記録再生器300の制御部301は、記録デバイスコントローラ303を介して記録デバイス400に初期化命令を送信する。これを受信した記録デバイス400は、記録デバイス暗号処理部401の制御部403において、通信部404を介して命令を受信し、認証フラグ2903をクリアする。すなわち未認証状態に設定する。または、記録再生器300から記録デバイス400に電源が供給される様な場合には、パワーオン時に未承認状態としてセットを行なう方式でもよい。

次に、記録再生器300の制御部301は、記録再生器暗号処理部302に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器300に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス400との認証処理、およびデータ送受信が可能となる。

初期化命令を受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の制御部において、記録デバイス挿入口番号に対応する認証フラグ2904をクリアする。すなわち未認証状態に設定する。

これらの初期化処理が完了すると、記録再生器300の制御部301は、記録デバイスコントローラ303を介してコマンド番号0から順次コマンド番号を昇順に出力する。記録デバイス400のコマンド番号管理部2901は、記録再生器300から入力されるコマンド番号を監視し、0から順次入力されることを確認して、対応するコマンドをコマンドレジスタ2902から取り出して認証処理等各種処理を実行する。入力されるコマンド番号が規定の順でなかった場合には、エラーとし、コマンド番号受付値を初期状態、すなわち実行可能コマンド番号=0にリセットする。

図29に示すようにコマンドレジスタ2902に格納されたコマンドシーケン

スは、認証処理を先行して処理するようにコマンド番号が付与されており、その後の処理に復号、鍵交換、暗号化処理の処理シーケンスが格納されている。

復号、鍵交換、暗号化処理の処理シーケンスの具体例を図30、31を用いて説明する。

図30は、先に図22において説明した記録再生器300から記録デバイス400へのコンテンツのダウンロード処理において実行される処理の一部を構成するものである。具体的には図22におけるステップS59～S60の間で実行される

図30において、ステップS3001は、記録再生器からセッション鍵 $K_{ses}$ で暗号化されたデータ（ex. ブロック情報鍵 $K_{bit}$ 、コンテンツ鍵 $K_{con}$ ）を記録デバイスが受信する処理であり、その後、前述の図29で示したコマンド列 $p \sim s$ が開始される。コマンド列 $p \sim s$ は認証処理コマンド0～kが完了し、図29に示す認証フラグ2903、2904に認証済みのフラグがセットされた後開始される。これは、コマンド番号管理部2901がコマンド番号を0から昇順でのみ受け付けることによって保証される。

ステップS3002は、記録デバイスが記録再生器から受信したセッション鍵 $K_{ses}$ で暗号化されたデータ（ex. ブロック情報鍵 $K_{bit}$ 、コンテンツ鍵 $K_{con}$ ）をレジスタに格納する処理である。

ステップS3003は、セッション鍵 $K_{ses}$ で暗号化されたデータ（ex. ブロック情報鍵 $K_{bit}$ 、コンテンツ鍵 $K_{con}$ ）をレジスタから取り出してセッション鍵 $K_{ses}$ で復号する処理を実行するステップである。

ステップS3004は、セッション鍵 $K_{ses}$ で復号化されたデータ（ex. ブロック情報鍵 $K_{bit}$ 、コンテンツ鍵 $K_{con}$ ）を保存鍵 $K_{str}$ で暗号化する処理を実行するステップである。

上記の処理ステップ3002～3004は、先の図29で説明したコマンドレジスタ中のコマンド番号 $p \sim s$ に含まれる処理である。これらの処理は、記録デバイス400のコマンド番号管理部2901において記録再生器300から受信

するコマンド番号  $p \sim s$  に従って記録デバイス暗号処理部 401 が順次実行する。

次のステップ S3005 は、保存鍵  $K_{str}$  で暗号化したデータ（ex. ブロック情報鍵  $K_{bit}$ 、コンテンツ鍵  $K_{con}$ ）を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部 401 から記録再生器 300 が保存鍵  $K_{str}$  で暗号化したデータを読み出して、その後に記録デバイス 400 の外部メモリ 402 に格納してもよい。

上述のステップ S3002～S3004 は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップ S3003 の復号処理終了時点で、記録再生器 300 からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ 2902 のコマンド番号  $p \sim s$  に設定された昇順のコマンド番号とは異なるため、コマンド番号管理部 2901 は、読み出しの実行を受け付けない。従って、記録デバイス 400 における鍵交換の際に発生する復号データを外部、例えば記録再生器 300 から読み出すことは不可能となり、鍵データ、コンテンツの不正な読み出しを防止できる。

図 31 は、先に図 28 において説明した記録デバイス 400 からコンテンツを読み出して記録再生器 300 において再生するコンテンツ再生処理において実行される処理の一部を構成するものである。具体的には図 28 におけるステップ S73 において実行される処理である。

図 31 において、ステップ S3101 は、記録デバイス 400 の外部メモリ 402 から保存鍵  $K_{str}$  で暗号化されたデータ（ex. ブロック情報鍵  $K_{bit}$ 、コンテンツ鍵  $K_{con}$ ）の読み出しを実行するステップである。

ステップ S3102 は、記録デバイスのメモリから読み出した保存鍵  $K_{str}$  で暗号化されたデータ（ex. ブロック情報鍵  $K_{bit}$ 、コンテンツ鍵  $K_{con}$ ）をレジスタに格納するステップである。このステップにおいては、記録デバイス 400 の外部メモリ 402 から記録再生器 300 が保存鍵  $K_{str}$  で暗号化したデータを読み出して、その後に記録デバイス 400 のレジスタに格納してもよ

い。

ステップS3103は、保存鍵K s t rで暗号化されたデータ（e x．ブロック情報鍵K b i t、コンテンツ鍵K c o n）をレジスタから取り出して保存鍵K s t rで復号処理するステップである。

ステップS3104は、保存鍵K s t rで復号化されたデータ（e x．ブロック情報鍵K b i t、コンテンツ鍵K c o n）をセッション鍵K s e sで暗号化処理するステップである。

上記の処理ステップ3102～3104は、先の図29で説明したコマンドレジスタ中のコマンド番号u～yに含まれる処理である。これらの処理は、記録デバイスのコマンド番号管理部2901において記録再生器300から受信するコマンド番号u～yに従って記録デバイス暗号処理部406が順次実行する。

次のステップS3105は、セッション鍵K s e sで暗号化したデータ（e x．ブロック情報鍵K b i t、コンテンツ鍵K c o n）を記録デバイスから記録再生器へ送信する処理である。

上述のステップS3102～S3104は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップS3103の復号処理終了時点で、記録再生器300からのデータ読み出し命令があつたとしても、その読み出しコマンドは、コマンドレジスタ2902のコマンド番号u～yに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部2901は、読み出しの実行を受け付けない。従って、記録デバイス400における鍵交換の際に発生する復号データを外部、例えば記録再生器300から読み出すことは不可能となり、鍵データあるいはコンテンツの不正な読み出しを防止できる。

なお、図30、31に示す処理では、鍵交換によって復号、暗号化される対象が、ブロック情報鍵K b i t、コンテンツ鍵K c o nである例を示したが、これらの図29に示したコマンドレジスタ2902に格納されたコマンドシーケンスには、コンテンツ自体の鍵交換を伴う復号、暗号化処理を含ませてもよく、鍵交換によって復号、暗号化される対象は上述の例に限定されるものではない。

以上、本発明のデータ処理装置における相互認証後の鍵交換処理について説明した。このように、本発明のデータ処理装置における鍵交換処理は、記録再生器と記録デバイス間での認証処理が終了した後においてのみ実行可能となり、さらに、鍵交換処理における復号データの外部からのアクセスが防止可能な構成となっているので、コンテンツ、鍵データの高度なセキュリティが確保される。

(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理

上述した実施例では、例えば図3に示すメディア500あるいは通信手段600におけるデータフォーマットが図4に示す1つの種類である場合について説明してきた。しかしながら、メディア500あるいは、通信手段600におけるデータフォーマットは、上述の図4に示すフォーマットに限らず、コンテンツが音楽である場合、画像データである場合、ゲーム等のプログラムである場合等、コンテンツに応じたデータフォーマットを採用することが望ましい。以下、複数の異なるデータデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理について説明する。

図32～35に4つの異なるデータフォーマットを示す。各図の左側には、図3に示すメディア500、または通信手段600上におけるデータフォーマットを、また各図の右側には記録デバイス400の外部メモリ402に格納される場合のデータフォーマットを示してある。先に、図32～35に示すデータフォーマットの概略を説明し、その後、各フォーマットにおける各データの内容、および各フォーマットにおけるデータの差異について説明する。

図32は、フォーマットタイプ0であり、上述の説明中で例として示したタイプと共通のものである。このフォーマットタイプ0の特徴は、データ全体を任意の大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割し、各ブロックについて任意に暗号化し、暗号化ブロックと非暗号化ブロック、すなわち平文ブロックを混在させてデータを構成できる点である。ブロックの暗号化は、コンテンツ鍵K<sub>con</sub>によって実行されており、コンテンツ鍵K<sub>con</sub>は、

メディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。ブロック情報鍵K b i tについてもメディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。これらの鍵交換は、前述の「(9) 相互認証後の鍵交換処理」において説明した処理にしたがって実行される。

図33は、フォーマットタイプ1であり、このフォーマットタイプ1は、フォーマットタイプ0と同様、データ全体をN個のデータブロック、すなわちブロック1～ブロックNに分割しているが、N個の各ブロックの大きさを同じ大きさとした点で前述のフォーマットタイプ0と異なる。コンテンツ鍵K c o nによるブロックの暗号化処理態様は前述のフォーマットタイプ0と同様である。また、メディア上で配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化されるコンテンツ鍵K c o nおよびブロック情報鍵K b i t構成も上述のフォーマットタイプ0と同様である。フォーマットタイプ1は、フォーマットタイプ0と異なり、固定的なブロック構成としたことで、ブロック毎のデータ長等の構成データが簡略化されるので、フォーマットタイプ0に比較してブロック情報のメモリサイズを減らすことが可能となる。

図33の構成例では、各ブロックを暗号化パートと非暗号化（平文）パートの1組によって構成している。このようにブロックの長さ、構成が規則的であれば、復号処理等の際に各ブロック長、ブロック構成を確認する必要がなくなるので効率的な復号、暗号処理が可能となる。なお、フォーマット1においては、各ブロックを構成するパート、すなわち暗号化パート、非暗号化（平文）パートは、各パート毎にチェック対象として定義可能な構成となっており、要チェックパーツを含むブロックである場合は、そのブロックに関してコンテンツチェック値I C V iが定義される。

図34は、フォーマットタイプ2であり、このフォーマットタイプ2の特徴は、同じ大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割され、各ブロックについて、それぞれ個別のブロック鍵 $K_{blc}$ で暗号化されていることである。各ブロック鍵 $K_{blc}$ の暗号化は、コンテンツ鍵 $K_{con}$ によって実行されており、コンテンツ鍵 $K_{con}$ は、メディア上では配送鍵 $K_{dis}$ によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 $K_{str}$ によって暗号化される。ブロック情報鍵 $K_{bit}$ についてもメディア上では配送鍵 $K_{dis}$ によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 $K_{str}$ によって暗号化される。

図35は、フォーマットタイプ3であり、このフォーマットタイプ3の特徴は、フォーマット・タイプ2と同様、同じ大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割され、各ブロックについて、それぞれ個別のブロック鍵 $K_{blc}$ で暗号化されていること、さらに、コンテンツ鍵を用いず、各ブロック鍵 $K_{blc}$ の暗号化は、メディア上では配送鍵 $K_{dis}$ によって暗号化され、記録デバイス上では保存鍵 $K_{str}$ によって暗号化されている点である。コンテンツ鍵 $K_{con}$ は、メディア上、デバイス上、いずれにも存在しない。ブロック情報鍵 $K_{bit}$ はメディア上では配送鍵 $K_{dis}$ によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 $K_{str}$ によって暗号化される。

次に、上記フォーマットタイプ0～3のデータの内容について説明する。データは先に説明したように、ヘッダ部とコンテンツ部に大きく2つに分類され、ヘッダ部にはコンテンツ識別子、取扱方針、チェック値A, B, 総チェック値、ブロック情報鍵、コンテンツ鍵、ブロック情報が含まれる。

取扱方針には、コンテンツのデータ長、ヘッダ長、フォーマットタイプ（以下説明するフォーマット0～3）、例えばプログラムであるか、データであるか等のコンテンツタイプ、前述のコンテンツの記録デバイスへのダウンロード、再生

の欄で説明したように、コンテンツが記録再生器固有に利用可能か否かを決定するフラグであるローカリゼーション・フラグ、さらに、コンテンツのコピー、ムーブ処理に関する許可フラグ、さらに、コンテンツ暗号化アルゴリズム、モード等、コンテンツに関する各種の利用制限情報および処理情報を格納する。

チェック値A : I C V a は、識別情報、取扱方針に対するチェック値であり、例えば、前述の図 2 3 で説明した手法によって生成される。

ブロック情報鍵 K b i t は、ブロック情報を暗号化するための鍵であり、先に説明したように、メディア上では配送鍵 K d i s によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 K s t r によって暗号化される。

コンテンツ鍵 K c o n は、コンテンツの暗号化に用いる鍵であり、フォーマットタイプ 0, 1 では、ブロック情報鍵 K b i t と同様にメディア上では配送鍵 K d i s によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 K s t r によって暗号化される。なお、フォーマットタイプ 2 では、コンテンツ鍵 K c o n は、コンテンツ各ブロックに構成されるブロック鍵 K b l c の暗号化にも利用される。また、フォーマット・タイプ 3 においては、コンテンツ鍵 K c o n は存在しない。

ブロック情報は、個々のブロックの情報を記述するテーブルであり、ブロックの大きさ、暗号化されているか否かについてのフラグ、すなわち各ブロックがチェックの対象 (I C V) と、なっているか否かを示す情報が格納される。ブロックがチェックの対象となっている場合は、ブロックのチェック値 I C V i (ブロック i のチェック値) がテーブル中に定義されて格納される。このブロック情報は、ブロック情報暗号鍵 K b i t によって暗号化される。

なお、ブロックのチェック値、すなわちコンテンツチェック値 I C V i は、ブロックが暗号化されている場合、平文 (復号文) 全体を 8 バイト単位で排他論理和した値を記録再生器 3 0 0 の内部メモリ 3 0 7 に格納されたコンテンツチェック値生成鍵 K i c v c で暗号化した値として生成される。また、ブロックが暗号

化されていない場合は、ブロックデータ（平文）の全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 $K_{icvc}$ を鍵とする）に入力して得た値として生成される。図36にコンテンツブロックのチェック値 $ICV_i$ を生成する構成例を示す。メッセージ $M$ の各々が復号文データまたは平文データの各8バイトを構成する。

なお、フォーマット・タイプ1においては、ブロック内のパーツのうち少なくとも1つがチェック値 $ICV_i$ の対象データ、すなわち要チェックパーツである場合は、そのブロックに関してコンテンツチェック値 $ICV_i$ が定義される。ブロック $i$ におけるパーツ $j$ のチェック値 $P-ICV_{ij}$ は、パーツ $j$ が暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵 $K_{icvc}$ で暗号化した値として生成される。また、パーツ $j$ が暗号化されていない場合は、パーツのブロックのデータ（平文）の全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 $K_{icvc}$ を鍵とする）に入力して得た値として生成される。

さらに、1つのブロック $i$ 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツ、すなわち要チェックパーツが1つのみ存在する場合は、上述の手法で生成したチェック値 $P-ICV_{ij}$ をそのままブロックのチェック値 $ICV_i$ とし、また、1つのブロック $i$ 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが複数存在する場合は、複数のパーツチェック値 $P-ICV_{ij}$ をパーツ番号順に連結したデータを対象にして8バイト単位で図37に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 $K_{icvc}$ を鍵とする）に入力して得た値として生成される。図37にコンテンツブロックのコンテンツチェック値 $ICV_i$ を生成する構成例を示す。

なお、フォーマット・タイプ2、3においては、ブロックのチェック値 $ICV_i$ は定義されない。

チェック値B : I C V b は、ブロック情報鍵、コンテンツ鍵、ブロック情報全体に対するチェック値であり、例えば、前述の図 2 4 で説明した手法によって生成される。

総チェック値 I C V t は、前述のチェック値A : I C V a、チェック値B : I C V b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 I C V i 全体に対するチェック値であり、前述の図 2 5 で説明したようにチェック値A : I C V a 等の各チェック値から生成される中間チェック値にシステム署名鍵 K s y s を適用して暗号化処理を実行することによって生成される。

なお、フォーマット・タイプ 2, 3 においては、総チェック値 I C V t は、前述のチェック値A : I C V a、チェック値B : I C V b にコンテンツデータ、すなわちブロック 1 のブロック鍵から最終ブロックまでのコンテンツデータ全体を連結したデータから生成される中間チェック値にシステム署名鍵 K s y s を適用して暗号化処理を実行することによって生成される。図 3 8 にフォーマット・タイプ 2, 3 における総チェック値 I C V t を生成する構成例を示す。

固有チェック値 I C V d e v は、前述のローカリゼーションフラグが 1 にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 I C V t に置き換えられるチェック値であり、フォーマット・タイプ 0, 1 の場合は、前述のチェック値A : I C V a、チェック値B : I C V b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 I C V i 全体に対するチェック値として生成される。具体的には、前述の図 2 5、または図 3 8 で説明したようにチェック値A : I C V a 等の各チェック値から生成される中間チェック値に記録再生器署名鍵 K d e v を適用して暗号化処理を実行することによって生成される。

次にフォーマットタイプ 0 ~ 3 各々における記録再生器 3 0 0 から記録デバイス 4 0 0 に対するコンテンツのダウンロード処理、および記録再生器 3 0 0 における記録デバイス 4 0 0 からの再生処理について図 3 9 ~ 4 4 のフローを用いて

説明する。

まず、フォーマットタイプ0, 1におけるコンテンツのダウンロード処理について図39を用いて説明する。

図39に示す処理は、例えば図3に示す記録再生器300に記録デバイス400を装着することによって開始される。ステップS101は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図20の認証処理フローに従って実行される。

ステップS101の認証処理が終了し、認証フラグがセットされると、記録再生器300は、ステップS102において、例えばコンテンツデータを格納したメディア500から、読み取り部304を介して所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信し、記録再生器300の制御部301が、データの内のヘッダ (Header) 部分を記録再生器300の記録再生器暗号処理部302に送信する。

次に、ステップS103において、暗号処理部302の制御部306が記録再生器暗号処理部302の暗号／復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵Kicvaを鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図7を用いて説明したICV計算方法に従って計算される。次に、ステップS104において、チェック値Aとヘッダ (Header) 内に格納されたチェック値: ICVaを比較し、一致していた場合にはステップS105へ進む。

先に説明したようにチェック値A, ICVaは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵Kicvaを鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして、例えばICV計算方法に従って計算されるチェック値Aが、ヘッダ (

Header) 内に格納されたチェック値: ICVaと一致した場合には、識別情報、取扱方針の改竄はないと判断される。

次に、ステップS105において、記録再生器暗号処理部302の制御部306は、配送鍵Kdisの取り出しまたは生成を記録再生器暗号処理部302の暗号／復号化部308に行わせる。配送鍵Kdisの生成方法は、先に説明した図22のステップS53と同様、例えば配送鍵用マスター鍵MKdisを用いて行われる。

次にステップS106において、記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号／復号化部308を使って、生成した配送鍵Kdisを用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵Kbitとコンテンツ鍵Kconの復号化処理を行う。

さらに、ステップS107において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308において、復号化したブロック情報鍵Kbitでブロック情報を復号化する。

さらに、ステップS108において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)から、チェック値B(ICVb')を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ(Header)内のICVbを比較し、一致していた場合にはステップS110へ進む。

先に説明したように、チェック値B、ICVbは、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値

B生成鍵 $K_{icvb}$ を鍵とし、ブロック情報鍵 $K_{bit}$ 、コンテンツ鍵 $K_{con}$ およびブロック情報（BIT）を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、ヘッダ（Header）内に格納されたチェック値： $ICV_b$ と一致した場合には、ブロック情報鍵 $K_{bit}$ 、コンテンツ鍵 $K_{con}$ 、ブロック情報の改竄はないと判断される。

ステップS110において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵 $K_{icvt}$ を鍵とし、検証したHeader内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7他で説明したICV計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。

次に、ステップS111において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に総チェック値 $ICV_t'$ の計算をさせる。総チェック値 $ICV_t'$ は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵 $K_{sys}$ を鍵とし、中間チェック値をDESで暗号化して生成する。次に、ステップS112において、生成した総チェック値 $ICV_t'$ とヘッダ（Header）内の $ICV_t$ を比較し、一致していた場合には、ステップS113へ進む。

先に図4において説明したように、総チェック値 $ICV_t$ は、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ（Header）内に格納されたチェック値： $ICV_t$ と一致した場合には、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

次に、ステップS113において、記録再生器300の制御部301は、プロ

ック情報（B I T）内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

コンテンツブロックが検証対象になっていた場合には、ステップS 1 1 4において、該当するコンテンツブロックを、記録再生器3 0 0の読み取り部3 0 4を使ってメディア5 0 0から読み出すか、記録再生器3 0 0の通信部3 0 5を使って通信手段6 0 0から受信し、記録再生器3 0 0の記録再生器暗号処理部3 0 2へ送信する。これを受信した記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にコンテンツチェック値I C V i' を計算させる。

コンテンツチェック値I C V i' は、先に説明したようにブロックが暗号化されている場合、コンテンツ鍵K c o nで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を全て8バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器3 0 0の内部メモリ3 0 7に格納されたコンテンツチェック値生成鍵K i c v cで暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を8バイト単位で図3 6に示す改竄チェック値生成関数（DES－CBC－MAC、コンテンツチェック値生成鍵K i c v cを鍵とする）に入力して得た値として生成される。

次にステップS 1 1 5において、記録再生器暗号処理部3 0 2の制御部3 0 6は、当該コンテンツチェック値と、ステップS 1 0 2で記録再生器3 0 0の制御部3 0 1から受信したコンテンツブロック内のI C Vを比較し、その結果を記録再生器3 0 0の制御部3 0 1に渡す。これを受信した記録再生器3 0 0の制御部3 0 1は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器3 0 0の記録再生器暗号処理部3 0 2に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す（ステップS 1 1 6）。

なお、ステップS 1 0 4、ステップS 1 0 9、ステップS 1 1 2、ステップS

115のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとしてダウンロード処理は終了する。

次に、ステップS117において、記録再生器300の記録再生器暗号処理部302は、ステップS106で復号化したブロック情報鍵Kbitとコンテンツ鍵Kconを、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵Ksesで暗号化させる。記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

次に、ステップS118において、記録再生器300から送信されてきたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再び暗号化させ、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵Kstrで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを読み出す。すなわち、配送鍵Kdisで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconの鍵のかけかえを行なう。

次に、ステップS119において、記録再生器300の制御部301は、データのヘッダ部の取扱方針(Usage Policy)から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できるか否かの判定を行なう。この判定は、ローカリゼーションフラグ(利用制限情報)=1に設定されている場合は、ダウンロードしたコンテンツが当該記録再生器300のみで利用でき、ローカリゼーションフラグ(利用制限情報)=0に設定されている場合は、ダウンロードしたコンテンツが別の同様な記録再生器300で

も利用できることを示す。判定の結果、ローカリゼーションフラグ（利用制限情報）＝１であった場合には、ステップＳ１２０に進む。

ステップＳ１２０において、記録再生器３００の制御部３０１は、記録再生器固有のチェック値を記録再生器３００の記録再生器暗号処理部３０２に計算させる。記録再生器固有のチェック値は、図２５に示すように記録再生器暗号処理部３０２の内部メモリ３０７に保存されている記録再生器に固有の記録再生器署名鍵Ｋ<sub>dev</sub>を鍵とし、ステップＳ１１０で生成した中間チェック値をＤＥＳで暗号化して生成する。計算された記録再生器固有のチェック値ＩＣＶ<sub>dev</sub>は、総チェック値ＩＣＶ<sub>t</sub>の代わりに上書きされる。

先に説明したように、システム署名鍵Ｋ<sub>sys</sub>は、配信システムに共通の署名またはＩＣＶをつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵Ｋ<sub>dev</sub>は、記録再生器毎に異なり、記録再生器が署名またはＩＣＶをつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵Ｋ<sub>sys</sub>によって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値ＩＣＶ<sub>t</sub>が一致することになるので、共通に利用可能となるが、記録再生器署名鍵Ｋ<sub>dev</sub>を用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Ｋ<sub>dev</sub>を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装置して再生しようとした場合、記録再生器固有のチェック値ＩＣＶ<sub>dev</sub>が不一致となり、エラーとなるので再生できないことになる。本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定できるものである。

次に、ステップＳ１２１において、記録再生器３００の制御部３０１は、記録再生器暗号処理部３０２に格納データフォーマットの形成を実行させる。先に説明したように、フォーマットタイプは０～３まで各タイプがあり、ヘッダ中の取扱方針（図５参照）中に設定され、この設定タイプにしたがって、先に説明した

図 3 2～3 5 の右側の格納フォーマットにしたがってデータを形成する。この図 3 9 に示すフローはフォーマット 0, 1 のいずれかであるので、図 3 2, 3 3 のいずれかのフォーマットに形成される。

ステップ S 1 2 1 において格納データフォーマットの形成が終了すると、ステップ 1 2 2 において、記録再生器 3 0 0 の制御部 3 0 1 は、コンテンツを記録デバイス 4 0 0 の外部メモリ 4 0 2 に保存する。

以上が、フォーマットタイプ 0, 1 におけるコンテンツデータのダウンロード処理の態様である。

次に、フォーマットタイプ 2 におけるコンテンツデータのダウンロード処理について図 4 0 を用いて説明する。上記したフォーマットタイプ 0, 1 のダウンロード処理と異なる点を中心に説明する。

ステップ S 1 0 1～S 1 0 9 は、上記したフォーマットタイプ 0, 1 のダウンロード処理と同様であるので説明は省略する。

フォーマットタイプ 2 は、先に説明したようにコンテンツチェック値  $ICV_i$  が定義されていないので、ブロック情報中には、コンテンツチェック値  $ICV_i$  を持たない。フォーマットタイプ 2 における中間チェック値は、図 3 8 に示すようにチェック値 A、チェック値 B と、第 1 ブロックの先頭データ（ブロック 1 のブロック鍵）から最終ブロックまでのコンテンツデータ全体を連結したデータに基づいて生成される中間チェック値にシステム署名鍵  $K_{sys}$  を適用して暗号化処理を実行することによって生成される。

従って、フォーマットタイプ 2 のダウンロード処理においては、ステップ S 1 5 1 においてコンテンツデータを読み出し、ステップ S 1 5 2 において、チェック値 A、チェック値 B と読み出したコンテンツデータに基づいて中間チェック値の生成を実行する。なお、コンテンツデータは暗号化されている場合でも、復号処理を行なわない。

フォーマットタイプ 2 では、前述のフォーマットタイプ 0, 1 での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、

迅速な処理が可能となる。

ステップS 1 1 1 以下の処理は、フォーマットタイプ0, 1における処理と同様であるので説明を省略する。

以上が、フォーマットタイプ2におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ2のダウンロード処理は、フォーマットタイプ0, 1での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

次に、フォーマットタイプ3におけるコンテンツデータのダウンロード処理について図4 1を用いて説明する。上記したフォーマットタイプ0, 1, 2のダウンロード処理と異なる点を中心に説明する。

ステップS 1 0 1～S 1 0 5は、上記したフォーマットタイプ0, 1, 2のダウンロード処理と同様であるので説明は省略する。

フォーマットタイプ3は、基本的にフォーマットタイプ2における処理と共通する部分が多いが、フォーマットタイプ3はコンテンツ鍵を有しておらず、またブロック鍵K b 1 cが記録デバイスにおいては保存鍵K s t rで暗号化されて格納される点がフォーマットタイプ2と異なる。

フォーマットタイプ3のダウンロード処理におけるフォーマットタイプ2と相違する点を中心として説明する。フォーマットタイプ3では、ステップS 1 0 5の次ステップであるステップS 1 6 1において、ブロック情報鍵の復号を行なう。記録再生器暗号処理部3 0 2の制御部3 0 6が、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8を使って、ステップS 1 0 5で生成した配送鍵K d i sを用いて、読み取り部3 0 4を介して受信したメディア5 0 0、または、通信部3 0 5を介して通信手段6 0 0から受信したデータのヘッダ部に格納されたブロック情報鍵K b i tの復号化処理を行う。フォーマットタイプ3では、データ中にコンテンツ鍵K c o nが存在しないため、コンテンツ鍵K c o nの復号化処理は実行されない。

次のステップS107では、ステップS161で復号したブロック情報鍵K b i tを用いてブロック情報の復号が実行され、さらに、ステップS162において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵K b i t、およびブロック情報（B I T）から、チェック値B（I C V b'）を生成する。チェック値Bは、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i t、およびブロック情報（B I T）からなる排他的論理和値をD E Sで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ（H e a d e r）内のI C V bを比較し、一致していた場合にはステップS151へ進む。

フォーマットタイプ3では、チェック値B、I C V bは、ブロック情報鍵K b i t、ブロック情報の改竄を検証するためのチェック値として機能する。生成したチェック値Bが、ヘッダ（H e a d e r）内に格納されたチェック値：I C V bと一致した場合には、ブロック情報鍵K b i t、ブロック情報の改竄はないと判断される。

ステップS151～S112は、フォーマットタイプ2の処理と同様であるので説明を省略する。

ステップS163では、ステップS151で読み出したコンテンツデータに含まれるブロック鍵K b l cをステップS105で生成した配送鍵K d i sによって復号する。

次にステップS164では、記録再生器300の記録再生器暗号処理部302が、ステップS161で復号化したブロック情報鍵K b i tと、ステップS163で復号したブロック鍵K b l cを、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵K s e sで暗号化させる。記録再生器300の制御部301は、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tとブロック鍵K b l cを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

次に、ステップS 1 6 5において、記録再生器3 0 0から送信されてきたブロック情報鍵K b i tとブロック鍵K b l cを受信した記録デバイス4 0 0は、受信したデータを記録デバイス暗号処理部4 0 1の暗号／復号化部4 0 6に、相互認証の際に共有しておいたセッション鍵K s e sで復号化させ、記録デバイス暗号処理部4 0 1の内部メモリ4 0 5に保存してある記録デバイス固有の保存鍵K s t rで再暗号化させ、記録再生器3 0 0の制御部3 0 1は、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介し、記録デバイス4 0 0から保存鍵K s t rで再暗号化されたブロック情報鍵K b i tとブロック鍵K b l cを読み出す。すなわち、当初、配送鍵K d i sで暗号化されたブロック情報鍵K b i tとブロック鍵K b l cを保存鍵K s t rで再暗号化されたブロック情報鍵K b i tとブロック鍵K b l cへ置き換えを行なう。

以下のステップS 1 1 9～S 1 2 2は、前述のフォーマットタイプ0, 1, 2と同様であるので説明を省略する。

以上が、フォーマットタイプ3におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ3のダウンロード処理は、フォーマットタイプ2と同様、ブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。また、ブロック鍵K b l cにより暗号化コンテンツを保護する範囲が局所化されているので、フォーマットタイプ2に比較して、よりセキュリティが高度となる。

次に、フォーマットタイプ0～3各々における記録再生器3 0 0における記録デバイス4 0 0からの再生処理について図4 2～4 5のフローを用いて説明する。

まず、フォーマットタイプ0におけるコンテンツの再生処理について図4 2を用いて説明する。

ステップS 2 0 1は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図2 0の認証処理フローに従って実行される。

ステップS 2 0 1の認証処理が終了し、認証フラグがセットされると、記録再生器3 0 0は、ステップS 2 0 2において、記録デバイス4 0 0から所定のフォーマットに従ったデータのヘッダを読み出し、記録再生器3 0 0の記録再生器暗号処理部3 0 2に送信する。

次に、ステップS 2 0 3において、暗号処理部3 0 2の制御部3 0 6が記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にチェック値Aを計算させる。チェック値Aは、先に説明した図2 3に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値A生成鍵K i c v aを鍵とし、識別情報 (C o n t e n t I D) と取扱方針 (U s a g e P o l i c y) をメッセージとして計算される。次に、ステップS 2 0 4において、計算されたチェック値Aとヘッダ (H e a d e r) 内に格納されたチェック値 : I C V a を比較し、一致していた場合にはステップS 2 0 5へ進む。

チェック値A, I C V a は、識別情報、取扱方針の改竄を検証するためのチェック値である。計算されたチェック値Aが、ヘッダ (H e a d e r) 内に格納されたチェック値 : I C V a と一致した場合には、記録デバイス4 0 0に格納された識別情報、取扱方針の改竄はないと判断される。

次に、ステップS 2 0 5において、記録再生器3 0 0の制御部3 0 1は、読み出したヘッダから記録デバイス固有の保存鍵K s t rで暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを取り出し、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介して記録デバイス4 0 0に送信する。

記録再生器3 0 0から送信されてきたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録デバイス4 0 0は、受信したデータを記録デバイス暗号処理部4 0 1の暗号／復号化部4 0 6に、記録デバイス暗号処理部4 0 1の内部メモリ4 0 5に保存してある記録デバイス固有の保存鍵K s t rで復号化処理させ、相互認証の際に共有しておいたセッション鍵K s e sで再び暗号化させる。この処理は、前述した(9)相互認証後の鍵交換処理の欄で詳しく述べた通りである。

ステップS206では、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを受信する。

次に、ステップS207において、記録再生器300の制御部301は、受信したセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302に送信し、セッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の暗号／復号化部308に、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを、相互認証の際に共有しておいたセッション鍵Ksesで復号化させる。

さらに、ステップS208において、復号化したブロック情報鍵Kbitで、ステップS202で読み出しておいたブロック情報を復号化する。なお、記録再生器300の記録再生器暗号処理部302は、復号化したブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITを、ステップS202で読み出したヘッダに含まれるブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITに置き換えて保持しておく。また、記録再生器300の制御部301は、復号化されたブロック情報BITを記録再生器300の記録再生器暗号処理部302から読み出しておく。

さらに、ステップS209において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)から、チェック値B(ICVb')を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS210において、チェック値Bとヘッダ

(Header) 内の I C V b を比較し、一致していた場合にはステップ S 2 1 1 へ進む。

チェック値 B, I C V b は、ブロック情報鍵 K b i t、コンテンツ鍵 K c o n、ブロック情報の改竄を検証するためのチェック値であり、生成したチェック値 B が、ヘッダ (Header) 内に格納されたチェック値: I C V b と一致した場合には、記録デバイス 4 0 0 に保存されたデータ中のブロック情報鍵 K b i t、コンテンツ鍵 K c o n、ブロック情報の改竄はないと判断される。

ステップ S 2 1 1 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に中間チェック値の計算をさせる。中間チェック値は、図 2 5 に示すように、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されている総チェック値生成鍵 K i c v t を鍵とし、検証した Header 内のチェック値 A、チェック値 B、ブロック情報中の全てのコンテンツチェック値をメッセージとして図 7 他で説明した I C V 計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に保持しておく。

次に、ステップ S 2 1 2 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録デバイス 4 0 0 の外部メモリ 4 0 2 から読み出したデータのヘッダ部に含まれる取扱方針 (U s a g e P o l i c y) から利用制限情報を取り出し、再生予定のコンテンツが当該記録再生器 3 0 0 のみで利用できる (利用制限情報が 1) か、別の同様な記録再生器 3 0 0 でも利用できる (利用制限情報が 0) か判定する。判定の結果、利用制限情報が 1、すなわち再生コンテンツが当該記録再生器 3 0 0 のみで利用できる利用制限が設定されている場合には、ステップ S 2 1 3 に進み、利用制限情報が 0、すなわち別の同様な記録再生器 3 0 0 でも利用できる設定であった場合には、ステップ S 2 1 5 に進む。なお、ステップ S 2 1 2 の処理は暗号処理部 3 0 2 が行なってもよい。

ステップ S 2 1 3 では、記録再生器 3 0 0 の制御部 3 0 1 は、記録再生器固有のチェック値 I C V d e v' を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2

に計算させる。記録再生器固有のチェック値  $ICV_{dev}'$  は、図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器署名鍵  $K_{dev}$  を鍵とし、ステップ S 211 で保持しておいた中間チェック値を DES で暗号化して生成する。

次に、ステップ S 214 において、ステップ S 213 で計算した記録再生器固有のチェック値  $ICV_{dev}'$  とステップ S 202 で読み出したヘッダ内の  $ICV_{dev}$  を比較し、一致していた場合には、ステップ S 217 へ進む。

一方ステップ S 215 では、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に総チェック値  $ICV_t$  の計算をさせる。総チェック値  $ICV_t'$  は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵  $K_{sys}$  を鍵とし、中間チェック値を DES で暗号化して生成する。次に、ステップ S 216 において、生成した総チェック値  $ICV_t'$  とヘッダ (Header) 内の  $ICV_t$  を比較し、一致していた場合には、ステップ S 217 へ進む。

総チェック値  $ICV_t$ 、および記録再生器固有のチェック値  $ICV_{dev}$  は、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成されたチェック値がヘッダ (Header) 内に格納されたチェック値： $ICV_t$  または  $ICV_{dev}$  と一致した場合には、記録デバイス 400 に格納された  $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

次に、ステップ S 217 において、記録再生器 300 の制御部 301 は、記録デバイス 400 からブロックデータを読み出す。さらに、ステップ S 218 において暗号化されているか否かを判定し、暗号化されている場合は、記録再生器 300 の暗号処理部 302 においてブロックデータの復号を行なう。暗号化されていない場合は、ステップ S 219 をスキップしてステップ S 220 に進む。

次に、ステップ S 220 において、記録再生器 300 の制御部 301 は、ブロック情報 (BIT) 内のコンテンツブロック情報に基づいて、コンテンツブロッ

クが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。コンテンツブロックが検証対象になっていた場合には、ステップS 2 2 1において、該当するコンテンツブロックのコンテンツチェック値  $ICV_i'$  を計算させる。コンテンツブロックが検証対象になっていない場合には、ステップS 2 2 1とS 2 2 2をスキップしてステップS 2 2 3に進む。

コンテンツチェック値  $ICV_i'$  は、先に図36で説明したようにブロックが暗号化されている場合、コンテンツ鍵  $K_{con}$  で、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を全て8バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器300の内部メモリ307に格納されたコンテンツチェック値生成鍵  $K_{icvc}$  で暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵  $K_{icvc}$  を鍵とする）に入力して得た値として生成される。

ステップS 2 2 2においては、記録再生器暗号処理部302の制御部306は、生成したコンテンツチェック値  $ICV_i'$  と、ステップS 2 0 2で記録デバイス400から受信したヘッダ部に格納されたコンテンツチェック値  $ICV_i$  とを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、ステップS 2 2 3において、記録再生器システムRAM上に実行（再生）用コンテンツ平文データを格納する。記録再生器300の制御部301は、さらに次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理、RAM格納処理を繰り返す（ステップS 2 2 4）。

なお、ステップS 2 0 4、ステップS 2 1 0、ステップS 2 1 4、ステップS 2 1 6、ステップS 2 2 2のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとして再生処理は終了する。

ステップS 2 2 4において全ブロック読み出しと判定されると、ステップS 2 2 5に進み、コンテンツ（プログラム、データ）の実行、再生が開始される。

以上が、フォーマットタイプ0におけるコンテンツデータの再生処理の態様である。

次に、フォーマットタイプ1におけるコンテンツデータの再生処理について図4 3を用いて説明する。上記したフォーマットタイプ0の再生処理と異なる点を中心に説明する。

ステップS 2 0 1～ステップS 2 1 7までの処理は、上記したフォーマットタイプ0の再生処理と同様であるので説明は省略する。

フォーマットタイプ1では、ステップS 2 3 1において、暗号化パーツの復号が実行され、パーツICVが生成される。さらに、ステップS 2 3 2において、ブロックICV $i'$ が生成される。先に説明したように、フォーマット・タイプ1においては、ブロック内のパーツのうち少なくとも1つがチェック値ICV $i$ の対象データである場合は、そのブロックに関してコンテンツチェック値ICV $i$ が定義される。ブロック $i$ におけるパーツ $j$ のチェック値P-ICV $i, j$ は、パーツ $j$ が暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵K $i, c, v, c$ で暗号化した値として生成される。また、パーツ $j$ が暗号化されていない場合は、データ（平文）全体を8バイト単位で図3 6に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵K $i, c, v, c$ を鍵とする）に入力して得た値として生成される。

さらに、1つのブロック $i$ 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが1つのみ存在する場合は、上述の手法で生成したチェック値P-ICV $i, j$ をそのままブロックのチェック値ICV $i$ とし、また、1つのブロック $i$ 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが複数存在する場合は、複数のパーツチェック値P-ICV $i, j$ をパーツ番号順に連結したデータ

を対象にしてデータ（平文）全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 $K_{icvc}$ を鍵とする）に入力して得た値として生成される。これは、先に図37で説明した通りである。

フォーマットタイプ1では、上述の手順で生成されたコンテンツチェック値の比較処理がステップS222で実行されることになる。以下のステップS223以下の処理はフォーマットタイプ0と同様であるので説明は省略する。

次に、フォーマットタイプ2におけるコンテンツデータの再生処理について図44を用いて説明する。上記したフォーマットタイプ0, 1の再生処理と異なる点を中心に説明する。

ステップS201～S210は、上記したフォーマットタイプ0, 1の再生処理と同様であるので説明は省略する。

フォーマットタイプ2においては、フォーマットタイプ0, 1において実行されたステップS211～S216の処理が実行されない。また、フォーマットタイプ2においては、コンテンツチェック値を持たないため、フォーマットタイプ0, 1において実行されたステップS222のコンテンツチェック値の検証も実行されない。

フォーマットタイプ2のデータ再生処理においては、ステップS210のチェック値Bの検証ステップの後、ステップS217に進み、記録再生器300の制御部301の制御によって、ブロックデータが読み出される。さらに、ステップS241において、記録再生器300の暗号処理部306によるブロックデータに含まれるブロック鍵 $K_{blc}$ の復号処理が実行される。記録デバイス400に格納されたブロック鍵 $K_{blc}$ は、図34で示すようにコンテンツ鍵 $K_{con}$ で暗号化されており、先のステップS207において復号したコンテンツ鍵 $K_{con}$ を用いてブロック鍵 $K_{blc}$ の復号を行なう。

次に、ステップS242において、ステップS241で復号されたブロック鍵 $K_{blc}$ を用いてブロックデータの復号処理が実行される。さらに、ステップS

243において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップS217～ステップS243の処理が全ブロックについて繰り返し実行される。ステップS244において全ブロック読み出しと判定されると再生処理は終了する。

このようにフォーマットタイプ2の処理は、総チェック値等のチェック値検証処理を省略しており、高速な復号処理の実行に適している構成であり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

次にフォーマットタイプ3におけるコンテンツデータの再生処理について図45を用いて説明する。上記したフォーマットタイプ0, 1, 2の再生処理と異なる点を中心に説明する。

フォーマットタイプ3は、基本的にフォーマットタイプ2における処理と共通する部分が多いが、フォーマットタイプ3は図35において説明したようにコンテンツ鍵を有しておらず、またブロック鍵Kb1cが記録デバイスにおいては保存鍵Kstrで暗号化されて格納される点がフォーマットタイプ2と異なる。

ステップS201～S210において、ステップS251、ステップS252、ステップS253、ステップS254の処理は、前述のフォーマットタイプ0, 1, 2における対応処理と異なりコンテンツ鍵を含まない処理として構成されている。

ステップS251において、記録再生器300の制御部301は、読み出したヘッダから記録デバイス固有の保存鍵Kstrで暗号化されたブロック情報鍵Kbitを取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

記録再生器300から送信されてきたブロック情報鍵Kbitを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで復号化処理させ、相互認証の際に共有しておいたセッション鍵Ksesで再暗号化させる。この処理は、前述した（9

) 相互認証後の鍵交換処理の欄で詳しく述べた通りである。

ステップS 2 5 2では、記録再生器3 0 0の制御部3 0 1は、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介し、記録デバイス4 0 0からセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tを受信する。

次に、ステップS 2 5 3において、記録再生器3 0 0の制御部3 0 1は、受信したセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tを記録再生器3 0 0の記録再生器暗号処理部3 0 2に送信し、セッション鍵K s e sで再暗号化されたブロック情報鍵K b i tを受信した記録再生器3 0 0の記録再生器暗号処理部3 0 2は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8に、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tを、相互認証の際に共有しておいたセッション鍵K s e sで復号化させる。

さらに、ステップS 2 0 8において、復号化したブロック情報鍵K b i tで、ステップS 2 0 2で読み出しておいたブロック情報を復号化する。なお、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、復号化したブロック情報鍵K b i tおよびブロック情報B I Tを、ステップS 2 0 2で読み出したヘッダに含まれるブロック情報鍵K b i tおよびブロック情報B I Tに置き換えて保持しておく。また、記録再生器3 0 0の制御部3 0 1は、復号化されたブロック情報B I Tを記録再生器3 0 0の記録再生器暗号処理部3 0 2から読み出しておく。

さらに、ステップS 2 5 4において、記録再生器暗号処理部3 0 2の制御部3 0 6は、ブロック情報鍵K b i tおよびブロック情報(B I T)から、チェック値B ( I C V b' ) を生成する。チェック値Bは、図2 4に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i tおよびブロック情報(B I T)からなる排他的論理和値をD E Sで暗号化して生成する。次に、ステップS 2 1 0において、チェック値Bとヘッダ(H e a d e r)内のI C V bを比較し、一致していた場合にはステップS 2 1 1へ進む。

フォーマットタイプ3では、さらに、ブロック鍵が記録デバイスでの格納時に

保存鍵によって暗号化されるため、記録デバイス400における保存鍵での復号処理、およびセッション鍵での暗号化処理、さらに、記録再生器300でのセッション鍵での復号処理が必要となる。これらの一連の処理がステップS255、ステップS256で示した処理ステップである。

ステップS255では、記録再生器300の制御部301は、ステップS217で読み出したブロックから記録デバイス固有の保存鍵K<sub>str</sub>で暗号化されたブロック鍵K<sub>blc</sub>を取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

記録再生器300から送信されてきたブロック鍵K<sub>blc</sub>を受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K<sub>str</sub>で復号化処理させ、相互認証の際に共有しておいたセッション鍵K<sub>ses</sub>で再暗号化させる。この処理は、前述した「(9) 相互認証後の鍵交換処理」の欄で詳しく述べた通りである。

ステップS256では、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵K<sub>ses</sub>で再暗号化されたブロック鍵K<sub>blc</sub>を受信する。

次に、ステップS257において、記録再生器300の暗号処理部306によるブロック鍵K<sub>blc</sub>のセッション鍵K<sub>ses</sub>を用いた復号処理が実行される。

次に、ステップS242において、ステップS257で復号されたブロック鍵K<sub>blc</sub>を用いてブロックデータの復号処理が実行される。さらに、ステップS243において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップS217～ステップS243の処理が全ブロックについて繰り返し実行される。ステップS244において全ブロック読み出しと判定されると再生処理は終了する。

以上の処理が、フォーマットタイプ3におけるコンテンツの再生処理である。総チェック値の検証処理が省略された点でフォーマットタイプ2と類似するが、

ブロック鍵の鍵交換処理を含む点でフォーマットタイプ2に比較して、さらにセキュリティ・レベルの高い処理構成となっている。

(11) コンテンツプロバイダにおけるチェック値 (ICV) 生成処理態様

上述の実施例中において、各種のチェック値 ICV についての検証処理が、コンテンツのダウンロード、または再生処理等の段階で実行されることを説明してきた。ここでは、これら各チェック値 (ICV) 生成処理、検証処理の態様について説明する。

まず、実施例で説明した各チェック値について、簡潔にまとめると、本発明のデータ処理装置において利用されるチェック値 ICV には以下のものがある。

チェック値A, ICV a : コンテンツデータ中の識別情報、取扱方針の改竄を検証するためのチェック値。

チェック値B, ICV b : ブロック情報鍵 K b i t、コンテンツ鍵 K c o n、ブロック情報の改竄を検証するためのチェック値。

コンテンツチェック値 ICV i : コンテンツの各コンテンツブロックの改竄を検証するためのチェック値。

総チェック値 ICV t : チェック値 ICV a、チェック値 ICV b、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。

再生器固有チェック値 ICV d e v : ローカリゼーションフラグが1にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 ICV t に置き換えられるチェック値であり、前述のチェック値A : ICV a、チェック値B : ICV b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 ICV i 全体に対するチェック値として生成される。

フォーマットによっては、ICV t、ICV d e v がチェックする対象に含まれるのは、各コンテンツブロックのチェック値ではなく、コンテンツそのものとなる場合もある。

以上の各チェック値が本発明のデータ処理装置において用いられる。上記各チ

チェック値の中で、チェック値A、チェック値B、総チェック値、コンテンツチェック値は、例えば図32～35、および図6に示されるようにコンテンツデータを提供するコンテンツプロバイダ、あるいはコンテンツ管理者によって、それぞれの検証対象データに基づいてICV値が生成され、コンテンツと共にデータ中に格納されて記録再生器300の利用者に提供される。記録再生器の利用者、すなわちコンテンツ利用者は、このコンテンツを記録デバイスにダウンロードする際、または再生する際にそれぞれの検証対象データに基づいて検証用のICVを生成して、格納済みのICVとの比較を行なう。また、再生器固有チェック値ICVdevは、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値ICVtに置き換えられて、記録デバイスに格納されるものである。

チェック値の生成処理は、前述の実施例中では、主としてDES-CBCによる生成処理構成を説明してきた。しかし、ICVの生成処理態様には、上述の方法に限らず様々な生成処理態様、さらに、様々な検証処理態様がある。特にコンテンツ提供者または管理者と、コンテンツ利用者との関係においては、以下に説明する各種のICV生成および検証処理構成が可能である。

図46～図48にチェック値ICVの生成者における生成処理と、検証者による検証処理を説明する図を示す。

図46は、上述の実施例中で説明したDES-CBCによるICVの生成処理を、例えばコンテンツ提供者または管理者であるICV生成者が行ない、生成したICVをコンテンツと共に記録再生器利用者、すなわち検証者に提供する構成である。この場合に記録再生器利用者、すなわち検証者が検証処理の際に必要な鍵は、例えば図18に示す内部メモリ307に格納された各チェック値生成鍵である。コンテンツ利用者である検証者（記録再生器利用者）は、内部メモリ307に格納されたチェック値生成鍵を使用して、検証対象のデータにDES-CBCを適用してチェック値を生成して格納チェック値と比較処理を実行する。この場合、各チェック値生成鍵は、ICVの生成者と、検証者が秘密に共有する

鍵として構成される。

図47は、コンテンツ提供者または管理者であるICVの生成者が公開鍵暗号系のデジタル署名によりICVを生成して、生成したICVをコンテンツと共にコンテンツ利用者、すなわち検証者に提供する。コンテンツ利用者、すなわち検証者は、ICV生成者の公開鍵を保存し、この公開鍵を用いてICVの検証処理を実行する構成である。この場合、コンテンツ利用者（記録再生器利用者）、すなわち検証者の有するICV生成者の公開鍵は秘密にする必要がなく、管理は容易となる。ICVの生成、管理が1つのエンティティにおいて実行される場合等、ICVの生成、管理が高いセキュリティ管理レベルで行われている場合に適した態様である。

図48は、コンテンツ提供者または管理者であるICVの生成者が公開鍵暗号系のデジタル署名によりICVを生成して、生成したICVをコンテンツと共にコンテンツ利用者、すなわち検証者に提供し、さらに、検証者が検証に用いる公開鍵を公開鍵証明書（例えば図14参照）に格納してコンテンツデータと共に記録再生器利用者、すなわち検証者に提供する。ICVの生成者が複数存在する場合には、各生成者は、公開鍵の正当性を証明するデータ（公開鍵証明書）を鍵管理センタに作成してもらう。

ICVの検証者であるコンテンツ利用者は、鍵管理センタの公開鍵を持ち、検証者は公開鍵証明書の検証を鍵管理センタの公開鍵によって実行し、正当性が確認されたら、その公開鍵証明書に格納されたICVの生成者の公開鍵を取り出す。さらに、取り出したICVの生成者の公開鍵を用いてICVの検証を実行する。

この方法は、ICVの生成者が複数あり、それらの管理を実行するセンタによる管理の実行システムが確立している場合に有効な態様である。

#### （12）マスタ鍵に基づく暗号処理鍵生成構成

次に、本発明のデータ処理システムにおける特徴的な構成の1つである、マスタ鍵に基づく各種暗号処理用鍵の生成構成について説明する。

先に図18を用いて説明したように、本発明のデータ処理装置における記録再生器300の内部メモリには、様々なマスタ鍵が格納され、これらの各マスタ鍵を用いて、例えば認証鍵K a k eを生成（数3参照）したり、あるいは配送鍵K d i sを生成（数4参照）する構成となっている。

従来、1対1のエンティティ間、すなわちコンテンツプロバイダとコンテンツ利用者間、あるいは、上述の本発明のデータ処理装置における記録再生器300と記録メディア400との間において暗号通信、相互認証、MAC生成、検証等を行なう際には、各エンティティに共通な秘密情報、例えば鍵情報を保持させていた。また、1対多の関係、例えば1つのコンテンツプロバイダに対する多数のコンテンツ利用者、あるいは1つの記録再生器に対する多数の記録メディア等の関係においては、すべてのエンティティ、すなわち多数のコンテンツ利用者、あるいは多数の記録メディアにおいて共有させた秘密情報、例えば鍵情報を格納保持させる構成とするか、あるいは、1つのコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報（e x . 鍵）を個別に管理し、これを各コンテンツ利用者に応じて使い分けていた。

しかしながら、上記のような1対多の利用関係がある場合、すべてが共有する秘密情報（e x . 鍵）を所有する構成においては、1箇所の秘密漏洩が発生すると同じ秘密情報（e x . 鍵）を利用している者すべてに影響が及ぶという欠点がある。また、1つの管理者、例えばコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報（e x . 鍵）を個別に管理し、これを各コンテンツ利用者に応じて使い分ける構成とすると、すべての利用者を識別し、かつその識別データに固有の秘密情報（e x . 鍵）を対応づけたリストが必要となり、利用者の増大に伴うリストの保守管理の負担が増加するという欠点がある。

本発明のデータ処理装置においては、このようなエンティティ間における秘密情報の共有における従来の問題点をマスター鍵の保有、およびマスター鍵から各種の個別鍵を生成する構成により解決した。以下、この構成について説明する。

本発明のデータ処理装置においては、記録デバイスやコンテンツを格納したメ

ディア、または記録再生器間での各種の暗号処理、認証処理等において異なる個別の鍵が必要になる場合、その個別の鍵を、デバイスやメディアが固有に持つ識別子データ（ID）などの個別情報と記録再生器300内であらかじめ決められた個別鍵生成方式を用いて生成する。この構成により万が一、生成された個別の鍵が特定された場合でもマスター鍵の漏洩を防止すれば、システム全体への被害を防ぐことが可能となる。またマスター鍵によって鍵を生成する構成により対応づけリストの管理も不要となる。

具体的な構成例について、図を用いて説明する。まず、図49に各種の鍵を記録再生器300の有する各種のマスタ鍵を用いて生成する構成を説明する図を示す。図49のメディア500、通信手段600からは、すでに説明した実施例と同様、コンテンツが入力される。コンテンツはコンテンツ鍵Kconによって暗号化され、またコンテンツ鍵Kconは、配送鍵Kdisによって暗号化されている。

例えば、記録再生器300がメディア500、通信手段600からコンテンツを取り出して、記録デバイス400にダウンロードしようとする場合、先の図2、図39～41において説明したように、記録再生器300は、コンテンツ鍵を暗号化している配送鍵Kdisを取得することが必要となる。このKdisをメディア500、通信手段600から直接取得したり、あるいは予め記録再生器300が取得して記録再生器300内のメモリに格納しておくことも可能であるが、このような鍵の多数のユーザに対する配布構成は、先にも説明したようにシステム全体に影響を及ぼす漏洩の可能性がある。

本発明のデータ処理システムでは、この配送鍵Kdisを図49の下部に示すように、記録再生器300のメモリに格納された配送鍵用マスター鍵MKdisと、コンテンツIDに基づく処理、すなわち $Kdis = DES(MKdis, \text{コンテンツID})$ を適用して配送鍵Kdisを生成する構成としている。本構成によれば、メディア500、通信手段600からコンテンツを供給するコンテンツプロバイダとそのコンテンツ利用者である記録再生器300間におけるコンテン

ツ配布構成において、コンテンツプロバイダが多数存在した場合であっても、個々の配送鍵  $K_{dis}$  をメディア、通信媒体等を介して流通させる必要もなく、また、各記録再生器 300 に格納する必要もなく、セキュリティを高度に保つことが可能となる。

次に、認証鍵  $K_{ake}$  の生成について説明する。先に説明した図 22、図 39～41 の記録再生器 300 から記録メディア 400 に対するダウンロード処理、あるいは図 28、図 42～45 で説明した記録メディア 400 に格納されたコンテンツを記録再生器 300 において実行、再生する場合、記録再生器 300 と記録メディア 400 間における相互認証処理（図 20 参照）が必要となる。

図 20 で説明したように、この認証処理において記録再生器 300 は認証鍵  $K_{ake}$  が必要となる。記録再生器 300 は、認証鍵を例えば記録メディア 400 から直接取得したり、あるいは予め記録再生器 300 が取得して記録再生器 300 内のメモリに格納しておくことも可能であるが、上述の配送鍵の構成と同様、このような鍵の多数のユーザに対する配布構成は、システム全体に影響を及ぼす漏洩の可能性がある。

本発明のデータ処理システムでは、この認証鍵  $K_{ake}$  を図 49 の下部に示すように、記録再生器 300 のメモリに格納された認証鍵用マスター鍵  $MK_{ake}$  と、記録デバイス識別  $ID: ID_{mem}$  に基づく処理、すなわち  $K_{ake} = DES(MK_{ake}, ID_{mem})$  によって認証鍵  $K_{ake}$  を求める構成としている。

さらに、図 22、図 39～41 の記録再生器 300 から記録メディア 400 に対するダウンロード処理、あるいは図 28、図 42～45 で説明した記録メディア 400 に格納されたコンテンツを記録再生器 300 において実行、再生する場合、記録再生器固有に利用可能なコンテンツである場合の記録再生器固有チェック値  $ICV_{dev}$  の生成処理に必要な記録再生器署名鍵  $K_{dev}$  についても上述の配送鍵、認証鍵と同様の構成とすることができる。上述の実施例中では、記録再生器署名鍵  $K_{dev}$  は内部メモリに格納する構成としていたが、記録再生

器署名鍵用マスター鍵 $MK_{dev}$ をメモリに格納し、記録再生器署名鍵 $K_{dev}$ は内部メモリに格納せず、必要に応じて図49の下部に示すように記録再生器識別子： $ID_{dev}$ と記録再生器署名鍵用マスター鍵 $MK_{dev}$ に基づいて、 $K_{dev} = DES(MK_{dev}, ID_{dev})$ によって記録再生器署名鍵 $K_{dev}$ を求める構成とすることで、記録再生器署名鍵 $K_{dev}$ を機器個別に持たせる必要がなくなるという利点が挙げられる。

このように、本発明のデータ処理装置においては、プロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような2つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各IDから逐次的に生成する構成としたので、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。

本構成に関する複数の処理例についてフローを示して説明する。図50は、コンテンツ製作または管理者におけるマスター鍵を用いたコンテンツ等の暗号化処理と、ユーザデバイス、例えば上述の実施例における記録再生器300におけるマスター鍵を用いた暗号化データの復号処理例である。

コンテンツ製作または管理者におけるステップS501は、コンテンツに対する識別子（コンテンツID）を付与するステップである。ステップS502は、コンテンツ製作または管理者の有するマスター鍵とコンテンツIDとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵 $K_{dis}$ を生成する工程とすれば、前述の $K_{dis} = DES(MK_{dis}, \text{コンテンツID})$ によって配送鍵 $K_{dis}$ を生成する。次に、ステップS503は、コンテンツの一部、または全部を鍵（例えば配送鍵 $K_{dis}$ ）によって暗号化するステップである。コンテンツ製作者は、このようなステップを経て暗号化処理を行なったコンテンツをDVD等のメディア、通信手段等を介して配信する。

一方、例えば記録再生器300等のユーザデバイス側では、ステップS504において、メディア、通信手段等を介して受領したコンテンツデータ中からコン

コンテンツIDを読み出す。次に、ステップS505において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵Kdisを得るものである場合は、例えば配送鍵 $Kdis = DES(MKdis, \text{コンテンツID})$ となる。ステップS506で、この鍵を用いてコンテンツを復号し、ステップS507で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

この例においては、図50下段に示すように、コンテンツ製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵MKdis）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ID（コンテンツID）に基づいて生成する。

このシステムでは、万が一配送鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、コンテンツIDの異なる他のコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

次に図51を用いて、コンテンツ製作または管理者が複数のマスター鍵を所有して、コンテンツの配信対象に応じた処理を実行する例について説明する。

コンテンツ製作または管理者におけるステップS511は、コンテンツに対する識別子（コンテンツID）を付与するステップである。ステップS512は、コンテンツ製作または管理者の有する複数のマスター鍵（例えば複数の配送鍵生成用マスター鍵MKdis）から1つのマスター鍵を選択するステップである。この選択処理は図52を用いてさらに説明するが、コンテンツの利用者の国ごと、機種ごと、あるいは機種のバージョンごとなどに対応付けて予め適用するマスター鍵を設定しておき、その設定に従って実行するものである。

次に、ステップS513では、ステップS512で選択したマスター鍵と、ステップS511で決定したコンテンツIDとに基づいて暗号化用の鍵を生成する

。これは例えば、配送鍵 $K_{disi}$ を生成する工程とすれば、 $K_{disi} = DES(MK_{disi}, \text{コンテンツID})$ によって生成する。次に、ステップS514はコンテンツの一部、または全部を鍵（例えば配送鍵 $K_{disi}$ ）によって暗号化するステップである。コンテンツ製作者は、ステップS515において、コンテンツIDと、使用したマスター鍵識別情報と、暗号化コンテンツを1つの配布単位として暗号化処理を行なったコンテンツをDVD等のメディア、通信手段等を介して配信する。

一方、例えば記録再生器300等のユーザデバイス側では、ステップS516において、DVD等のメディア、通信手段等を介して配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有するか否かについて判定する。コンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を持たない場合は、その配布コンテンツは、そのユーザデバイスにおいては利用できないものであり、処理は終了する。

配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有する場合は、ステップS517において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツIDを読み出す。次に、ステップS518において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 $K_{disi}$ を得るものである場合は、例えば配送鍵 $K_{disi} = DES(MK_{disi}, \text{コンテンツID})$ となる。ステップS519で、この鍵を用いてコンテンツを復号し、ステップS520で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

この例においては、図51下段に示すように、コンテンツ製作または管理者は、複数のマスター鍵、例えば複数の配送鍵生成用マスター鍵 $MK_{dis1} \sim n$ からなるマスター鍵セットを有する。一方、ユーザデバイスには1つのマスター鍵例えば1つの配送鍵生成用マスター鍵 $KK_{disi}$ を有し、コンテンツ製作または管理者が $MK_{disi}$ を用いて暗号化処理している場合のみ、ユーザデバイス

は、そのコンテンツを復号して利用することができる。

この図51のフローに示す態様の具体例として、国毎に異なるマスター鍵を適用した例を図52に示す。コンテンツプロバイダは、マスター鍵MK1～nを有し、MK1は日本向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いる。例えば、コンテンツIDとMK1から暗号化鍵K1を生成してK1によってコンテンツを暗号化する。また、MK2はUS向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用い、MK3はEU（ヨーロッパ）向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いるよう設定している。

一方、日本向けユーザデバイス、具体的には日本で販売されるPCまたはゲーム機器等の記録再生器には、マスター鍵MK1がその内部メモリに格納され、US向けユーザデバイスには、マスター鍵MK2がその内部メモリに格納され、EU向けユーザデバイスには、マスター鍵MK3がその内部メモリに格納されている。

このような構成において、コンテンツプロバイダは、コンテンツを利用可能なユーザデバイスに応じて、マスター鍵MK1～nから、マスター鍵を選択的に使用してユーザデバイスに配信するコンテンツの暗号化処理を実行する。例えばコンテンツを日本向けのユーザデバイスのみ利用可能とするためには、マスター鍵MK1を用いて生成された鍵K1によってコンテンツを暗号化する。この暗号化コンテンツは、日本向けユーザデバイスに格納されたマスター鍵MK1を用いて復号可能、すなわち復号鍵を生成可能であるが、他のUS、またはEU向けのユーザデバイスに格納されたマスター鍵MK2、MK3からは鍵K1を得ることができないので、暗号化コンテンツの復号は不可能となる。

このように、コンテンツプロバイダが複数のマスター鍵を選択的に使用することにより、様々なコンテンツの利用制限を設定することができる。図52では、ユーザデバイスの国別にマスター鍵を区別する例を示したが、前述のように、ユーザデバイスの機種に応じて、あるいはバージョンに応じてマスター鍵を切り換

える等、様々な利用形態が可能である。

次に、図53にメディア固有の識別子、すなわちメディアIDとマスター鍵を組み合わせた処理例を示す。ここで、メディアとは例えばDVD、CD等のコンテンツを格納したメディアである。メディアIDは、1つ1つのメディアごとに固有としてもよいし、たとえば、映画などのコンテンツのタイトルごとに固有としてもよいし、メディアの製造ロットごとに固有としてもよい。このようにメディアIDの割り当て方法としては様々な方法を用いることができる。

メディア製作または管理者におけるステップS521は、メディアに対する識別子（メディアID）を決定するステップである。ステップS522は、メディア製作または管理者の有するマスター鍵とメディアIDとに基づいてメディア内の格納コンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵 $K_{dis}$ を生成する工程とすれば、前述の $K_{dis} = DES(MK_{dis}, \text{メディアID})$ によって配送鍵 $K_{dis}$ を生成する。次に、ステップS523は、メディア格納コンテンツの一部、または全部を鍵（例えば配送鍵 $K_{dis}$ ）によって暗号化するステップである。メディア製作者は、このようなステップを経て暗号化処理を行なったコンテンツ格納メディアを供給する。

一方、例えば記録再生器300等のユーザデバイス側では、ステップS524において、供給されたメディアからメディアIDを読み出す。次に、ステップS525において、読み出したメディアIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 $K_{dis}$ を得るものである場合は、例えば配送鍵 $K_{dis} = DES(MK_{dis}, \text{メディアID})$ となる。ステップS526で、この鍵を用いてコンテンツを復号し、ステップS527で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

この例においては、図53下段に示すように、メディア製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵 $MK_{dis}$ ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有

するマスター鍵と各ID（メディアID）に基づいて生成する。

このシステムでは、万が一メディア鍵が第三者に漏洩した場合、そのメディア内のコンテンツの復号が第三者において可能となるが、メディアIDの異なる他のメディアに格納されたコンテンツの復号は防止することが可能であるため、1つのメディア鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、メディア毎の鍵の対応付けリストを保持する必要がないという効果もある。また、1つのメディア鍵で暗号化されるコンテンツサイズは、そのメディア内に格納可能な容量に制限されるため、暗号文攻撃のために必要な情報量に達する可能性は少なく、暗号解読の可能性を低減させることができる。

次に、図54に記録再生器固有の識別子、すなわち記録再生器IDとマスター鍵を組み合わせた処理例を示す。

記録再生器利用者におけるステップS531は、記録再生器の例えば内部メモリに格納されたマスター鍵と記録再生器IDとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、コンテンツ鍵 $K_{con}$ を生成する工程とすれば、 $K_{con} = DES(MK_{con}, \text{記録再生器ID})$ によってコンテンツ鍵 $K_{con}$ を生成する。次に、ステップS532は、格納するコンテンツの一部、または全部を鍵（例えば配送鍵 $K_{con}$ ）によって暗号化するステップである。ステップS533は、暗号化コンテンツを例えばハードディスク等の記録デバイスに格納する。

一方、記録再生器を管理するシステム管理者側では、コンテンツを格納した記録再生器利用者から格納データの復旧を依頼されると、ステップS534において、記録再生器から、記録再生器IDを読み出す。次に、ステップS535において、読み出した記録再生器IDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、コンテンツ鍵 $K_{con}$ を得るものである場合は、例えばコンテンツ鍵 $K_{con} = DES(MK_{con}, \text{記録再生器ID})$ となる。ステップS536で、この鍵を用いてコンテンツを復号

する。

この例においては、図 5 4 下段に示すように、記録再生器利用者と、システム管理者の双方がマスター鍵（例えばコンテンツ鍵生成用マスター鍵MK c o n）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各 I D（記録再生器 I D）に基づいて生成する。

このシステムでは、万が一コンテンツ鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、記録再生器 I D の異なる他の記録再生器用に暗号化されたコンテンツの復号は防止することが可能であるため、1 つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、システム管理側、ユーザデバイス側両者において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

図 5 5 は、スレーブデバイス、例えばメモリカード等の記録デバイスと、ホストデバイス、例えば記録再生器間における相互認証処理に用いる認証鍵をマスター鍵に基づいて生成する構成である。先に説明した認証処理（図 2 0 参照）では、スレーブデバイスの内部メモリに認証鍵を予め格納した構成としてあるが、これを図 5 5 に示すように認証処理時にマスター鍵に基づいて生成する構成とすることができる。

例えば記録デバイスであるスレーブデバイスは、認証処理開始前の初期化处理として、ステップ S 5 4 1 において、記録デバイスであるスレーブデバイスの内部メモリに格納したマスター鍵とスレーブデバイス I D とに基づいて相互認証処理に用いる認証鍵 K a k e を生成する。これは例えば、 $K a k e = DES (MK a k e, \text{スレーブデバイス I D})$  によって生成する。次に、ステップ S 5 4 2 において、生成した認証鍵をメモリに格納する。

一方、例えば記録再生器等のホストデバイス側では、ステップ S 5 4 3 において、装着された記録デバイス、すなわちスレーブデバイスから、通信手段を介してスレーブデバイス I D を読み出す。次に、ステップ S 5 4 4 において、読み出したスレーブデバイス I D と所有する認証鍵生成用マスター鍵に基づいて相互認

証処理に適用する認証鍵を生成する。この生成処理は、例えば認証鍵  $K_{ake} = DES(MK_{ake}, \text{スレーブデバイスID})$  となる。ステップ S545 で、この認証鍵を用いて認証処理を実行する。

この例においては、図 55 下段に示すように、スレーブデバイスと、マスターデバイスの双方がマスター鍵、すなわち認証鍵生成用マスター鍵  $MK_{ake}$  を有し、相互認証処理に必要な認証鍵を逐次的にそれぞれの所有するマスター鍵とスレーブデバイス ID に基づいて生成する。

このシステムでは、万が一認証鍵が第三者に漏洩した場合、その認証鍵は、そのスレーブデバイスのみ有効であるため、他のスレーブデバイスとの関係においては、認証が成立しないことになり、鍵の漏洩によって発生する影響を最小限にすることができるという効果がある。

このように、本発明のデータ処理装置においては、コンテンツプロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような 2 つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各 ID から逐次的に生成する構成とした。従って、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。

### (13) 暗号処理における暗号強度の制御

上述した実施例において、記録再生器 300 と記録デバイス 400 間での暗号処理は、説明を理解しやすくするため、主として、先に図 7 を用いて説明したシングル DES 構成による暗号処理を用いた例について説明してきた。しかしながら、本発明のデータ処理装置において適用される暗号化処理方式は上述したシングル DES 方式に何ら限定されるものではなく、必要なセキュリティ状態に応じた暗号化方式を採用することが可能である。

例えば先に説明した図 8 ～ 図 10 の構成のようなトリプル DES 方式を適用してもよい。例えば図 3 に示す記録再生器 300 の暗号処理部 302 と、記録デバイス 400 の暗号処理部 401 の双方において、トリプル DES 方式を実行可能

な構成とし、図 8～図 10 で説明したトリプルDES方式による暗号処理に対応する処理を実行する構成が可能である。

しかしながら、コンテンツの提供者は、コンテンツに応じて処理速度を優先してコンテンツ鍵K<sub>con</sub>をシングルDES方式による64ビット鍵構成とする場合もあり、また、セキュリティを優先してコンテンツ鍵K<sub>con</sub>をトリプルDES方式による128ビット、または192ビット鍵構成とする場合もある。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の構成をトリプルDES方式、シングルDES方式いずれか一方の方式のみ対応可能な構成とすることは好ましくない。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401は、シングルDES、トリプルDESいずれの方式にも対応可能とする構成が望ましい。

しかしながら、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の暗号処理構成をシングルDES方式、トリプルDES方式の双方を実行可能な構成とするためには、それぞれの別の回路、ロジックを構成しなければならない。例えば、記録デバイス400においてトリプルDESに対応する処理を実行するためには、先の図29に示すコマンドレジスタにトリプルDESの命令セットを新たに格納することが必要となる。これは記録デバイス400に構成する処理部の複雑化を招くこととなる。

そこで、本発明のデータ処理装置は、記録デバイス400側の暗号処理部401の有するロジックをシングルDES構成として、かつトリプルDES暗号化処理に対応した処理が実行可能で、トリプルDES方式による暗号化データ(鍵、コンテンツ等)を記録デバイスの外部メモリ402に格納することを可能とした構成を提案する。

例えば図32に示すデータフォーマットタイプ0の例において、記録再生器300から記録デバイス400に対してコンテンツデータのダウンロードを実行する際、先に説明したフォーマットタイプ0のダウンロードのフローを示す図39のステップS101で認証処理を実行し、ここでセッション鍵K<sub>ses</sub>を生成す

る。さらに、ステップS 1 1 7において、記録再生器3 0 0側の暗号処理部3 0 2においてセッション鍵K s e sによるコンテンツ鍵K c o nの暗号化処理が実行され、この暗号化鍵が記録デバイス4 0 0に通信手段を介して転送され、ステップS 1 1 8において、この暗号化鍵を受信した記録デバイス4 0 0の暗号処理部4 0 3がセッション鍵K s e sによるコンテンツ鍵K c o nの復号処理を実行し、さらに、保存鍵K s t rによるコンテンツ鍵K c o nの暗号化処理を実行して、これを記録再生器3 0 0の暗号処理部3 0 2に送信し、その後、記録再生器3 0 0がデータフォーマットを形成（ステップS 1 2 1）してフォーマット化されたデータを記録デバイス4 0 0に送信し、記録デバイス4 0 0が受信したデータを外部メモリ4 0 2に格納する処理を行なっている。

上記処理においてステップS 1 1 7，S 1 1 8間において実行される記録デバイス4 0 0の暗号処理部4 0 1での暗号処理をシングルDES、またはトリプルDESいずれかの方式を選択的に実行可能な構成とすれば、コンテンツ提供者がトリプルDESにしたがったコンテンツ鍵K c o nを用いたコンテンツデータを提供する場合も、またシングルDESにしたがったコンテンツ鍵K c o nを用いたコンテンツデータを提供する場合も、いずれの場合にも対応可能となる。

図5 6に本発明のデータ処理装置における記録再生器3 0 0の暗号処理部3 0 2と、記録デバイス4 0 0の暗号処理部4 0 1との双方を用いてトリプルDES方式に従った暗号処理方法を実行する構成を説明するフローを示す。図5 6では、一例として記録再生器3 0 0からコンテンツデータを記録デバイス4 0 0にダウンロードする際に実行される保存鍵K s t rを用いたコンテンツ鍵K c o nの暗号化処理例であり、コンテンツ鍵K c o nがトリプルDES方式による鍵である場合の例を示している。なお、ここでは、コンテンツ鍵K c o nを代表して、その処理例を示すが、他の鍵、またはコンテンツ等、その他のデータについても同様の処理が可能である。

トリプルDES方式においては、先の図8～1 0において説明したように、シングルDESでは6 4ビット鍵、トリプルDES方式による場合は、1 2 8ビッ

ト、または192ビット鍵構成として、2つ、または3つの鍵が用いられる処理である。これら3つのコンテンツ鍵をそれぞれKcon1, Kcon2, (Kcon3)とする。Kcon3は用いられない場合もあるので、かっこで示している。

図56の処理について説明する。ステップS301は記録再生器300と、記録デバイス400間での相互認証処理ステップである。この相互認証処理ステップは、先に説明した図20の処理によって実行される。なお、この認証処理の際、セッション鍵Ksesが生成される。

ステップS301の認証処理が終了すると、ステップS302において、各チェック値、チェック値A、チェック値B、コンテンツチェック値、総チェック値、各ICVの照合処理が実行される。

これらのチェック値(ICV)照合処理が終了し、データ改竄がないと判定されると、ステップS303に進み、記録再生器300において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308を使って、先に取り出したまたは生成した配送鍵Kdisを用いて、受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたコンテンツ鍵Kconの復号化処理を行う。この場合のコンテンツ鍵は、トリプルDES方式による鍵であり、コンテンツ鍵Kcon1, Kcon2, (Kcon3)である。

次に、ステップS304において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon1のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。

記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたコンテンツ鍵Kcon1を含むデータを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコント

ローラ 303 を介して記録デバイス 400 に送信する。

次に、ステップ S 305 において、記録再生器 300 から送信されてきたコンテンツ鍵 K c o n 1 を受信した記録デバイス 400 は、受信したコンテンツ鍵 K c o n 1 を記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵 K s e s で復号化する。さらに、ステップ S 306 において、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵 K s t r で再暗号化させて、通信部 404 を介して記録再生器 300 に送信する。

次に、ステップ S 307 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 において、ステップ S 303 で復号化したコンテンツ鍵 K c o n 1, K c o n 2, (K c o n 3) の中のコンテンツ鍵 K c o n 2 のみを相互認証の際に共有しておいたセッション鍵 K s e s で暗号化する。

記録再生器 300 の制御部 301 は、セッション鍵 K s e s で暗号化されたコンテンツ鍵 K c o n 2 を含むデータを記録再生器 300 の記録再生器暗号処理部 302 から読み出し、これらのデータを記録再生器 300 の記録デバイスコントローラ 303 を介して記録デバイス 400 に送信する。

次に、ステップ S 308 において、記録再生器 300 から送信されてきたコンテンツ鍵 K c o n 2 を受信した記録デバイス 400 は、受信したコンテンツ鍵 K c o n 2 を記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵 K s e s で復号化する。さらに、ステップ S 309 において、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵 K s t r で再暗号化させて、通信部 404 を介して記録再生器 300 に送信する。

次に、ステップ S 310 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 において、ステップ S 303 で復号化したコンテンツ鍵 K c o n 1, K c o n 2, (K c o n 3) の

中のコンテンツ鍵  $K_{con3}$  のみを相互認証の際に共有しておいたセッション鍵  $K_{ses}$  で暗号化する。

記録再生器 300 の制御部 301 は、セッション鍵  $K_{ses}$  で暗号化されたコンテンツ鍵  $K_{con3}$  を含むデータを記録再生器 300 の記録再生器暗号処理部 302 から読み出し、これらのデータを記録再生器 300 の記録デバイスコントローラ 303 を介して記録デバイス 400 に送信する。

次に、ステップ S311 において、記録再生器 300 から送信されてきたコンテンツ鍵  $K_{con3}$  を受信した記録デバイス 400 は、受信したコンテンツ鍵  $K_{con3}$  を記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵  $K_{ses}$  で復号化する。さらに、ステップ S312 において、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵  $K_{str}$  で再暗号化させて、通信部 404 を介して記録再生器 300 に送信する。

次にステップ S313 において、記録再生器の暗号処理部は、図 32～35 で説明した各種のデータフォーマットを形成して、記録デバイス 400 に送信する。

最後にステップ S314 において、記録デバイス 400 は、フォーマット形成が終了した受信データを外部メモリ 402 に格納する。このフォーマットデータには、保存鍵  $K_{str}$  で暗号化されたコンテンツ鍵  $K_{con1}$ ,  $K_{con2}$ , ( $K_{con3}$ ) を含んでいる。

このような処理を実行することにより、記録デバイス 400 に格納するコンテンツ鍵をトリプル DES 方式の暗号方式による鍵として格納することが可能となる。なお、コンテンツ鍵が  $K_{con1}$ ,  $K_{con2}$  の 2 つの鍵である場合は、ステップ S310～S312 の処理は省略される。

このように、記録デバイス 400 は、同じ態様の処理、すなわちステップ S305, S306 の処理ステップを複数回、その対象を変更するのみで繰り返し実行することにより、トリプル DES の適用された鍵をメモリに格納可能となる。

コンテンツ鍵K c o nがシングルD E Sの適用鍵である場合は、ステップS 3 0 5, S 3 0 6を実行して、ステップS 3 1 3のフォーマット化処理を実行してメモリに格納すればよい。このような構成は、ステップS 3 0 5, S 3 0 6の処理を実行するコマンドを先に説明した図29のコマンドレジスタに格納し、この処理をコンテンツ鍵の態様、すなわちトリプルD E S方式か、シングルD E S方式かによって、適宜1回～3回実行する構成とすればよい。従って、記録デバイス400の処理ロジック中にトリプルD E Sの処理方式を含ませることなく、トリプルD E S方式、シングルD E S方式、の双方の処理が可能となる。なお、暗号化方式については、コンテンツデータのヘッダ部内の取扱方針に記録し、これを参照することで判定することが可能である。

#### (14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理

先に説明した図4～6のコンテンツデータ構成から理解されるように、本発明のデータ処理装置において利用されるコンテンツデータのヘッダ部に格納された取扱方針には、コンテンツタイプ、起動優先順位情報が含まれる。本発明のデータ処理装置における記録再生器300は、記録デバイス400、あるいは、D V D、C D、ハードディスク、さらにはゲームカートリッジ等の各種記録媒体に記録されたアクセス可能なコンテンツデータが複数存在する場合、これらコンテンツの起動順位を起動優先順位情報に従って決定する。

記録再生器300は、各記録デバイスD V D装置、C Dドライブ装置、ハードディスクドライブ装置等各種記録デバイスとの認証処理を実行後、コンテンツデータ中の優先順位情報に従って、最も優先順位の高いコンテンツデータ中のプログラムを優先して実行する。以下、この「コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」について説明する。

上述した本発明のデータ処理装置実施例の説明においては、記録再生器300が1つの記録デバイス400からコンテンツデータを再生、実行する場合の処理を中心として説明した。しかし、一般に記録再生器300は、図2に示すように

記録デバイス 400 の他に、読み取り部 304 を介して DVD、CD、ハードディスク、さらに、PIO111、SIO112 を介して接続されるメモリカード、ゲームカートリッジ等、各種記録媒体にアクセス可能な構成を有する。なお、図 2 では、図の複雑化を避けるため読み取り部 304 を 1 つのみ記載しているが、記録再生器 300 は、異なる記憶媒体、例えば DVD、CD、フロッピーディスク、ハードディスクを並列に装着可能である。

記録再生器 300 は、複数の記憶媒体にアクセス可能であり、それぞれの記憶媒体にはそれぞれコンテンツデータが格納されている。例えば CD 等外部のコンテンツプロバイダが供給するコンテンツデータは、前述の図 4 のデータ構成でメディアに格納され、これらのメディアまたは、通信手段を介してダウンロードした場合には、図 26、図 27 のコンテンツデータ構成でメモリカード等の各記憶媒体に格納されている。さらに、具体的には、コンテンツデータのフォーマットタイプに応じて図 32～35 に示すようにメディア上、記録デバイス上でそれぞれ異なるフォーマットで格納される。しかし、いずれの場合にもコンテンツデータのヘッダ中の取扱方針にはコンテンツタイプ、起動優先順位情報が含まれる。

これら、複数のコンテンツデータに対するアクセスが可能な場合の記録再生器のコンテンツ起動処理をフローに従って説明する。

図 57 は、起動可能コンテンツが複数ある場合の処理例 (1) を示す処理フローである。ステップ S611 は、記録再生器 300 がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能な記録デバイスには、メモリカード、DVD 装置、CD ドライブ、ハードディスク装置、さらに、例えば PIO111、SIO112 を介して接続されるゲームカートリッジ等が含まれる。認証処理は、図 2 で示す制御部 301 の制御のもとに各記録デバイスに対して例えば先に図 20 で説明した手順に従って実行される。

次に、ステップ S612 おいて、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラム

であるものを抽出する処理として実行される。

次に、ステップS 6 1 3において、ステップS 6 1 2で抽出された起動可能なプログラムにおける起動優先順位を判定する。これは、具体的には、ステップS 6 1 2において選択された複数の起動可能なコンテンツデータのヘッダ中の取扱情報に含まれる優先情報を比較して最も高い優先順位を選択する処理である。

次にステップS 6 1 4で選択されたプログラムを起動する。なお、複数の起動可能なプログラムにおいて設定された優先順位が同じである場合には、記録デバイス間でデフォルトの優先順位を設定し、最優先されるデバイスに格納されたコンテンツプログラムを実行する。

図5 8には、複数の記録デバイスに識別子を設定し、各識別子の付された記録デバイスについて順次、認証処理、コンテンツプログラム検索を実行する処理態様、すなわち起動可能コンテンツが複数ある場合の処理例(2)を示した。

ステップS 6 2 1では、記録再生器3 0 0に装着された記録デバイス(i)の認証処理(図2 0参照)を実行するステップである。複数(n個)の記録デバイスには順次1~nの識別子が付与されている。

ステップS 6 2 2では、ステップS 6 2 1での認証が成功したか否かを判定し、認証が成功した場合は、ステップS 6 2 3に進み、その記録デバイス(i)の記録媒体中から起動可能プログラムを検索する。認証が成功しなかった場合は、ステップS 6 2 7に進み、新たなコンテンツ検索可能な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS 6 2 8に進み記録デバイス識別子iを更新し、ステップS 6 2 1以降の認証処理ステップを繰り返す。

ステップS 6 2 3における処理は、記録デバイス(i)に格納されたコンテンツデータから起動可能なプログラムを検出する処理である。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

ステップS 6 2 4では、コンテンツタイプがプログラムであるものが抽出され

たか否かを判定し、抽出された場合は、ステップS 6 2 5において、抽出プログラム中最も優先順位の高いものを選択し、ステップS 6 2 6において選択プログラムを実行する。

ステップS 6 2 4において、コンテンツタイプがプログラムであるものが抽出されなかったと判定された場合には、ステップS 6 2 7に進み、新たなコンテンツ検索な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS 6 2 8に進み記録デバイス識別子*i*を更新し、ステップS 6 2 1以降の認証処理ステップを繰り返す。

図59は、起動可能コンテンツが複数ある場合の処理例(3)を示す処理フローである。ステップS 6 5 1は、記録再生器300がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能なDVD装置、CDドライブ、ハードディスク装置、メモリカード、ゲームカートリッジ等の認証処理を実行する。認証処理は、図2で示す制御部301の制御のもとに各記録デバイスに対して例えば先に図20で説明した手順に従って実行される。

次に、ステップS 6 5 2において、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

次に、ステップS 6 5 3において、ステップS 6 5 2で抽出された起動可能なプログラムの名称等の情報を表示手段に表示する。なお、表示手段は図2では示されていないが、AV出力データとして出力されたデータが図示しない表示手段に出力される構成となっている。なお、各コンテンツデータのプログラム名等のユーザ提供情報は、コンテンツデータの識別情報中に格納されており、図2に示すメインCPU106の制御のもとに制御部301を介して認証済みの各コンテンツデータのプログラム名称等、プログラム情報を出力手段に出力する。

次にステップS 6 5 4では、図2に示す入力インタフェース、コントローラ、マウス、キーボード等の入力手段からのユーザによるプログラム選択入力を入力

インタフェース 110 を介してメイン CPU 106 が受領し、選択入力にしたがって、ステップ S 655 においてユーザ選択プログラムを実行する。

このように本発明のデータ処理装置では、コンテンツデータ中のヘッダ内の取扱情報にプログラム起動優先順位情報を格納し、記録再生器 300 がこの優先順位に従ってプログラムを起動する、あるいは表示手段に起動プログラム情報を表示してユーザによって選択する構成としたので、ユーザがプログラムを検索する必要がなく、起動に要する時間およびユーザの労力を省くことが可能となる。また、起動可能なプログラムは、すべて記録デバイスの認証処理後に起動、または起動可能プログラムであることの表示がなされるので、プログラムを選択してから正当性の確認を行なう等の処理の煩雑性が解消される。

#### (15) コンテンツ構成および再生（伸長）処理

本発明のデータ処理装置では、上述したように記録再生器 300 は、メディア 500 または通信手段 600 からコンテンツをダウンロード、あるいは記録デバイス 400 から再生処理を行う。上記の説明は、コンテンツのダウンロード、あるいは再生処理に伴う、暗号化データの処理を中心として説明してきた。

図 3 の記録再生器 300 における制御部 301 は、コンテンツデータを提供する DVD 等のデバイス 500、通信手段 600、記録デバイスからのコンテンツデータのダウンロード処理、または再生処理に伴う認証処理、暗号化、復号化処理全般を制御する。

これらの処理結果として得られた再生可能なコンテンツは、例えば音声データ、画像データ等である。復号データは制御部 301 から図 2 に示すメイン CPU の制御下に置かれ、音声データ、画像データ等に応じて AV 出力部に出力される。しかし、コンテンツが例えば音声データであって MP3 圧縮がなされていれば、図 2 に示す AV 出力部の MP3 デコーダによって音声データの復号処理がなされて出力される。また、コンテンツデータが画像データであり、MPEG2 圧縮画像であれば、AV 処理部の MPEG2 デコーダによって伸長処理が実行されて出力されることになる。このように、コンテンツデータに含まれるデータは、圧

縮（符号化）処理がなされている場合もあり、また圧縮処理の施されていないデータもあり、コンテンツに応じた処理を施して出力する。

しかしながら、圧縮処理、伸長処理プログラムには、様々な種類があり、コンテンツプロバイダから圧縮データを提供されても対応する伸長処理実行プログラムが無い場合は、これを再生することができないという事態が発生する。

そこで、本発明のデータ処理装置は、データコンテンツ中に、圧縮データとその復号（伸長）処理プログラムを併せて格納する構成、あるいは圧縮データと復号（伸長）処理プログラムとのリンク情報をコンテンツデータのヘッダ情報として格納する構成を開示する。

図 2 に示したデータ処理全体図から、本構成に関する要素および関連要素を簡潔にまとめた図を図 6 0 に示す。記録再生器 3 0 0 は、例えば DVD、CD 等のデバイス 5 0 0、または通信手段 6 0 0、あるいはコンテンツを格納したメモリカード等の記録デバイス 4 0 0 から様々なコンテンツの提供を受ける。これらのコンテンツは、音声データ、静止画像、動画像データ、プログラムデータ等であり、また暗号化処理の施されているもの、施されていないもの、また、圧縮処理がなされているもの、なされていないもの等、様々なデータが含まれる。

受領コンテンツが暗号化されている場合は、すでに上述した項目中で説明したような手法によって制御部 3 0 1 の制御、および暗号処理部 3 0 2 の暗号処理によって復号処理が実行される。復号されたデータはメイン CPU 1 0 6 の制御下で、AV 処理部に 1 0 9 に転送されて、AV 処理部 1 0 9 のメモリ 3 0 9 0 に格納された後、コンテンツ解析部 3 0 9 1 においてコンテンツ構成の解析が実行される。例えばコンテンツ中にデータ伸長プログラムが格納されていれば、プログラム記憶部 3 0 9 3 にプログラムを格納し、音声データ、画像データ等のデータが含まれていればこれらをデータ記憶部 3 0 9 2 に記憶する。伸長処理部 3 0 9 4 では、プログラム記憶部に記憶された例えば MP 3 等の伸長処理プログラムを用いてデータ記憶部 3 0 9 2 に記憶された圧縮データの伸長処理を実行して、スピーカ 3 0 0 1、モニタ 3 0 0 2 に出力される。

次に、AV処理部109が制御部301を介して受領するデータの構成および処理のいくつかの例について説明する。なお、ここでは、コンテンツの例として音声データを示し、また圧縮プログラムの例としてMP3を適用したものを代表して説明するが、本構成は、音声データのみならず、画像データにも適用できるものであり、また、圧縮伸長処理プログラムについてもMP3のみならず、MP EG 2, 4等各種のプログラムを適用することが可能である。

図61にコンテンツ構成例を示す。図61はMP3によって圧縮された音楽データ6102、MP3復号(伸長)処理プログラム6101を併せて1つのコンテンツとして構成した例である。これらのコンテンツは、1コンテンツとしてメディア500、あるいは記録デバイス400に格納され、または通信手段600から配信される。記録再生器300は、これらのコンテンツが先に説明した通り、暗号化されているものであれば、暗号処理部303によって復号処理を実行した後、AV処理部109に転送される。

AV処理部109のコンテンツ解析部3091では、受け取ったコンテンツを解析し、音声データ伸長プログラム(MP3デコーダ)部と、圧縮音声データ部からなるコンテンツから、音声データ伸長プログラム(MP3デコーダ)部を取り出してプログラム記憶部3093にプログラムを記憶し、圧縮音声データをデータ記憶部3092に記憶する。なお、コンテンツ解析部3091は、コンテンツとは別に受領したコンテンツ名、コンテンツ構成情報等の情報を受領したり、あるいはコンテンツ内に含まれるデータ名等の識別データ、データ長、データ構成等を示すデータに基づいてコンテンツ解析を実行してもよい。次に、圧縮伸長処理部3094は、プログラム記憶部3093に記憶された音声データ伸長プログラム(MP3デコーダ)に従ってデータ記憶部3092に記憶されたMP3圧縮音声データの伸長処理を実行して、AV処理部109は伸長した音声データをスピーカ3001に出力する。

図62に図61のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS671は、AV処理部109のメモリ3090に格納された

データ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のデータから取り出し、モニタ 3002 に表示する。ステップ S 672 は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース 110 を介して受領し、CPU 106 の制御のもとにユーザ入力データに基づく再生処理命令を AV 処理部 109 に出力する。AV 処理部 109 は、ステップ S 673 においてユーザ選択によるデータの抽出、伸長処理を実行する。

次に図 63 に、1 つのコンテンツには圧縮音声データ、あるいは伸長処理プログラムのいずれか一方が含まれ、さらに各コンテンツのヘッダ情報としてコンテンツの内容を示すコンテンツ情報が含まれる構成例を示す。

図 63 に示すように、コンテンツがプログラム 6202 である場合は、ヘッダ情報 6201 としてプログラムであること、およびプログラム種類が MP3 伸長プログラムであることを示すコンテンツ識別情報が含まれる。一方、音声データ 6204 をコンテンツとして含む場合は、ヘッダ 6203 のコンテンツ情報には MP3 圧縮データであるとの情報が含まれる。このヘッダ情報は、前述した例えば図 4 に示すコンテンツデータ構成の取扱方針（図 5 参照）中に含まれるデータから再生に必要な情報のみを選択して AV 処理部 109 へ転送するコンテンツに付加して構成することが可能である。具体的には、図 5 に示す「取扱方針」中の各構成データに暗号処理部 302 において必要となる取扱方針データと、AV 処理部 109 における再生処理時に必要となるデータとの識別値を付加し、これら識別値が、AV 処理部 109 において必要であることを示すもののみを抽出してヘッダ情報とすることができる。

図 63 に示す各コンテンツを受領した AV 処理部 109 のコンテンツ解析部 3091 は、ヘッダ情報に従って、プログラムである場合はプログラムコンテンツをプログラム記憶部 3093 に記憶し、データである場合は、データコンテンツをデータ記憶部 3092 に記憶する。その後、圧縮伸長処理部 3094 は、データ記憶部からデータを取り出して、プログラム記憶部 3093 に記憶した MP3

プログラムに従って伸長処理を実行して出力する。なお、プログラム記憶部 3093 にすでに同一プログラムが格納されている場合は、プログラム格納処理は省略してもよい。

図 64 に図 63 のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップ S675 は、AV 処理部 109 のメモリ 3090 に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のヘッダから取り出し、モニタ 3002 に表示する。ステップ S676 は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース 110 を介して受領する。

次に、ステップ S677 では、ユーザ選択に対応するデータの再生用プログラム（例えば MP3）を検索する。このプログラム検索対象は、記録再生機器 300 のアクセス可能な範囲を最大検索範囲とすることが好ましく、例えば図 60 に示す、各メディア 500、通信手段 600、記録デバイス 400 等も検索範囲とする。

AV 処理部 109 に渡されるコンテンツはデータ部のみであり、プログラムコンテンツは記録再生器 300 内の他の記録媒体に格納される場合もあり、DVD、CD 等のメディアを介してコンテンツ提供者から提供されることもある。従って、検索対象を記録再生機器 300 のアクセス格納範囲を検索範囲とする。検索の結果として再生プログラムが見つかり、CPU 106 の制御のもとにユーザ入力データに基づく再生処理命令を AV 処理部 109 に出力する。AV 処理部 109 は、ステップ S679 においてユーザ選択によるデータの抽出、伸長処理を実行する。また、別の実施例として、プログラムの検索をステップ S675 より前に行い、ステップ S675 においては、プログラムが検出されたデータのみを表示するようにしてもよい。

次に図 65 に、1 つのコンテンツに圧縮音声データ 6303、伸長処理プログラム 6302 が含まれ、さらにコンテンツのヘッダ情報 6301 としてコンテンツの再生優先順位情報が含まれる構成例を示す。これは、先の図 61 のコンテン

ツ構成にヘッダ情報として再生優先順位情報を付加した例である。これは、前述の「(14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」と同様、AV処理部109が受領したコンテンツ間において設定された再生優先順位に基づいて再生順を決定するものである。

図66に図65のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS681は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS682において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択し、ステップS683において、選択されたデータの再生処理を実行する。

次に図67に、1つのコンテンツにヘッダ情報とプログラムデータ6402、あるいはヘッダ情報6403と、圧縮データ6404のいずれかの組合せから成る例において、データコンテンツのヘッダ6403にのみ、再生優先順位情報が付加されている構成例を示す。

図68に図67のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS691は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS692において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択する。

次に、ステップS693では、選択されたデータに対応するデータ再生用プログラム（例えばMP3）を検索する。このプログラム検索対象は、先の図64のフローにおける処理と同様、記録再生機器300のアクセス格納範囲を最大検索範囲とすることが好ましく、例えば図60に示す各メディア500、通信手段600、記録デバイス400等も検索範囲とする。

検索の結果として再生プログラムが見つかる（ステップS694でYes）と

、ステップS 6 9 5において、選択されたデータを検索の結果得られたプログラムを用いて、伸長再生処理を実行する。

一方、検索結果としてプログラムが検出されなかった場合（ステップS 6 9 4でY e s）は、ステップS 6 9 6に進み、ステップS 6 9 1で設定した検索リスト中に含まれる他のデータにおいて、同一のプログラムを用いた再生処理が必要なものを削除する。これは、新たにそのデータに対する再生プログラム検索を実行しても検出されないことが明らかであるからである。さらに、ステップS 6 9 7において検索リストが空であるかを判定し、からでない場合は、ステップS 6 9 2に戻り、さらに次の優先順位の高いデータを抽出して、プログラム検索処理を実行する。

このように、本構成によれば、圧縮処理されたコンテンツは、その復号（伸長）プログラムと共に構成されるか、あるいはコンテンツが圧縮されたデータのみ、あるいは伸長処理プログラムのみである場合は、それぞれのコンテンツにコンテンツがどのような圧縮データであるのか、あるいはどのような処理を実行するかを示すヘッダ情報を有しているので、コンテンツを受領した処理部（例えばA V処理部）は、圧縮データに付属する伸長処理プログラムを用いて伸長再生処理を実行するか、あるいは伸長処理プログラムを圧縮データのヘッダ情報に基づいて検索して、検索の結果得られたプログラムにしたがって伸長再生処理を実行するので、ユーザによるデータの伸長プログラムの選択、検索等の処理が不要となりユーザ負担が軽減され、効率的なデータ再生が可能となる。さらに、ヘッダに再生優先順位情報を有した構成によれば、再生順序を自動設定する構成が可能となり、ユーザによる再生順設定の操作を省略することができる。

なお、上述の実施例では、圧縮音声データコンテンツ、および音声圧縮データの伸長処理プログラムとしてのMP 3を例として説明したが、圧縮データを含むコンテンツ、圧縮画像データの伸長処理プログラムを有するコンテンツであっても本構成は同様に適用可能であり、同様の効果を奏するものである。

（1 6）セーブデータの生成および記録デバイスへの格納、再生処理

本発明のデータ処理装置は、例えば記録再生器 300 において実行されるコンテンツがゲームプログラム等である場合等、ゲームプログラムを途中で中断して、所定時間後、新たに再開したい場合には、その中断時点のゲーム状態等をセーブ、すなわち記録デバイスに格納し、これを再開時に読み出してゲームを続行することが可能な構成を持つ。

従来のゲーム機器、パソコン等の記録再生器におけるセーブデータ保存構成は、例えば記録再生器に内蔵、あるいは外付け可能なメモ리카ード、フロッピーディスク、ゲームカートリッジ、あるいはハードディスク等の記憶媒体にセーブデータを保存する構成を持つが、特に、そのセーブデータに対するセキュリティ確保構成を有しておらず、例えばゲームアプリケーションプログラムに共通の仕様でデータのセーブ処理が行われる構成となっている。

従って、例えばある 1 つの記録再生器 A を用いてセーブされたセーブデータが別のゲームプログラムによって使用されたり、書換えられたりする事態が発生し、従来、セーブデータのセキュリティはほとんど考慮されていなかったのが実状である。

本発明のデータ処理装置は、このようなセーブデータのセキュリティ確保を実現可能とした構成を提供する。例えばあるゲームプログラムのセーブデータは、そのゲームプログラムのみが使用可能な情報に基づいて暗号化して記録デバイスに格納する。あるいは、記録再生器固有の情報に基づいて暗号化して記録デバイスに格納する。これらの手法により、セーブデータの利用を特定の機器、特定のプログラムのみに制限することができ、セーブデータのセキュリティが確保される。以下、本発明のデータ処理装置における「セーブデータの生成および記録デバイスへの格納、再生処理」について説明する。

図 69 に本発明のデータ処理装置におけるセーブデータ格納処理について説明するブロック図を示す。DVD、CD等のメディア 500、あるいは通信手段 600 からコンテンツが記録再生器 300 に提供される。提供されるコンテンツは、先に説明したようにコンテンツ固有の鍵であるコンテンツ鍵  $K_{con}$  によって

暗号化されており、記録再生器 300 は、前述した「(7) 記録再生器から記録デバイスへのダウンロード処理」の欄で説明 (図 22 参照) した処理に従ってコンテンツ鍵を取得して、暗号化コンテンツを復号した後、記録デバイス 400 に格納する。ここでは、記録再生器 300 がコンテンツプログラムをメディア、通信手段から復号して再生、実行を行ない、実行の後、得られるセーブデータを外付け、あるいは内蔵のメモリカード、ハードディスク等の各種の記録デバイス 400 A、400 B、400 C のいずれかに格納し、再生する処理、あるいはコンテンツを記録デバイス 400 A にダウンロードした後、記録デバイス 400 A からコンテンツを再生、実行して、そのセーブデータを外付け、あるいは内蔵のメモリカード、ハードディスク等の各種の記録デバイス 400 A、400 B、400 C のいずれかに格納する処理記録デバイス 400 に格納し、再生する処理について説明する。

記録再生器 300 には、先に説明したように記録再生器識別子  $IDdev$ 、システムに共通な署名鍵であるシステム署名鍵  $Ksys$ 、個々の記録再生器に固有の署名鍵である記録再生器署名鍵  $Kdev$ 、さらに各種の個別鍵を生成するマスタ鍵を有する。マスタ鍵については、「(12) マスタ鍵に基づく暗号処理鍵生成構成」において、詳しく説明した通り、例えば、配送鍵  $Kdis$ 、あるいは認証鍵  $Kake$  等を生成する鍵である。ここでは、特にマスタ鍵の種類を限定することなく記録再生器 300 の有するマスタ鍵全般を代表するものとして  $MKx$  として示す。図 69 の下段には、セーブデータの暗号鍵  $Ksav$  の例を示した。セーブデータ暗号鍵  $Ksav$  は、セーブデータを各種記録デバイス 400 A～C に格納する場合の暗号化処理、そして、各種記録デバイス 400 A～C から再生する際の復号処理に用いられる暗号鍵である。図 70 以下を用いて、セーブデータの格納処理および再生処理の例を説明する。

図 70 は、コンテンツ個有鍵、システム共通鍵のいずれかを用いてセーブデータを記録デバイス 400 A～C いずれかに格納する処理のフロー図である。なお、各フローにおける処理は記録再生器 300 が実行する処理であり、各フローで

セーブデータを格納する記録デバイスは内蔵、外付け記録デバイス400A～Cのいずれかであればよく、いずれかに限定されるものではない。

ステップS701は、コンテンツ識別子、例えばゲームIDを記録再生器300が読み出す処理である。これは、先に説明した図4、26、27、32～35に示すコンテンツデータ中の識別情報に含まれるデータであり、セーブデータの格納処理命令を図2に示す入力インタフェース110を介して受領したメインCPU106がコンテンツ識別子の読み取りを制御部301に指示する。

制御部301は、実行プログラムがDVD、CD-ROM等、読取部304を介して実行されているコンテンツの場合は、読取部304を介してコンテンツデータ中のヘッダに含まれる識別情報を取り出し、実行プログラムが、記録デバイス400に格納されたコンテンツである場合は、記録デバイスコントローラ303を介して識別情報を取り出す。なお、記録再生器300がコンテンツプログラムを実行中で、すでに記録再生器中のRAM、その他のアクセス可能な記録媒体にコンテンツ識別子が格納済みである場合は、新たな読み取り処理を実行せずに、読み込み済みデータに含まれる識別情報を利用してもよい。

次に、ステップS702は、プログラムの使用制限を行なうか否かによって処理を変更するステップである。プログラム使用制限とは、保存するセーブデータをそのプログラムのみに固有に利用可能とする制限を付するか否かを設定する制限情報であり、プログラムのみに固有に利用可能とする場合は、「プログラム使用制限あり」とし、プログラムに利用を拘束されないセーブデータとする場合を「プログラム使用制限なし」とする。これは、ユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよく、設定された制限情報は、図69の記録デバイス400A～Cにデータ管理ファイルとして格納される。

データ管理ファイルの例を図71に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象と

なったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図69に示す[IDdev]である。プログラム使用制限は、上述したように保存するセーブデータをそのプログラムのみに固有に利用可能とす場合、「する」の設定とし、対応プログラムに制限されない利用を可能とする場合「しない」の設定となる。プログラム使用制限は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

図70に戻り、フローの説明を続ける。ステップS702において、プログラム使用制限について「する」の設定がされている場合は、ステップS703に進む。ステップS703では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵Kconを読み出してコンテンツ固有鍵をセーブデータ暗号鍵Ksavとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ暗号鍵Ksavを生成する。

一方、ステップS702において、プログラム使用制限について「しない」の設定がされている場合は、ステップS707に進む。ステップS707では、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵Ksysを記録再生器300の内部メモリ307から読み出して、システム署名鍵Ksysをセーブデータ暗号鍵Ksavとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

次に、ステップS704において、ステップS703、またはステップS707で選択、または生成されたセーブデータ暗号化鍵Ksavを用いてセーブデータの暗号化処理を実行する。この暗号化処理は、図2における暗号処理部302が例えば前述のDESアルゴリズムを適用して実行する。

ステップS704において暗号化処理されたセーブデータは、ステップS70

5において記録デバイスに格納される。セーブデータを格納可能な記録デバイスが図69に示すように複数ある場合は、ユーザが記録デバイス400A~Cのいずれかをセーブデータ格納先として予め選択する。さらに、ステップS706において先に図71を用いて説明したデータ管理ファイルに先にステップS702で設定したプログラム使用制限情報の書き込み、すなわちプログラム使用制限「する」または「しない」の書き込みを実行する。

以上で、セーブデータの格納処理が終了する。ステップS702においてYes、すなわち「プログラム使用制限する」の選択がなされ、ステップS703においてコンテンツ固有鍵に基づいて生成されたセーブデータ暗号化鍵Ksavによって暗号化処理されたセーブデータは、コンテンツ固有鍵情報を持たないコンテンツプログラムによる復号処理が不可能となり、セーブデータは同じコンテンツ鍵情報を有するコンテンツプログラムのみが利用できることになる。ただし、ここでは、セーブデータ暗号化鍵Ksavは記録再生器固有の情報に基いて生成されたものではないので、例えばメモリカード等の着脱可能な記録デバイスに格納されたセーブデータは異なる記録再生器においても対応するコンテンツプログラムと共に使用する限り再生可能となる。

また、ステップS702においてNo、すなわち「プログラム使用制限しない」の選択がなされ、ステップS707においてシステム共通鍵に基づくセーブデータ暗号化鍵Ksavによって暗号化処理されたセーブデータは、コンテンツ識別子が異なるプログラムを用いた場合でも、また、記録再生器が異なっていた場合でも再生して利用することが可能となる。

図72は、図70のセーブデータ格納処理によって格納されたセーブデータを再生する処理を示したフローである。

ステップS711は、コンテンツ識別子、例えばゲームIDを記録再生器300が読み出す処理である。これは、先に説明した図70のセーブデータ格納処理のステップS701と同様の処理であり、コンテンツデータ中の識別情報に含まれるデータを読み出す処理である。

次に、ステップS 7 1 2では、図6 9に示す記録デバイス4 0 0 A～Cから、図7 1を用いて説明したデータ管理ファイルを読み出し、ステップS 7 1 1において読み出したコンテンツ識別子、および対応して設定された使用プログラム制限情報を抽出する。データ管理ファイルに設定されたプログラム使用制限が「する」であった場合は、ステップS 7 1 4に進み、「しない」であった場合には、ステップS 7 1 7に進む。

ステップS 7 1 4では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵K c o nを読み出してコンテンツ固有鍵をセーブデータ復号化鍵K s a vとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ復号化鍵K s a vを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

一方、ステップS 7 1 2において、データ管理ファイルの設定がプログラム使用制限について「しない」の設定であった場合は、ステップS 7 1 7において、記録再生器3 0 0内に格納されたシステム共通鍵、例えばシステム署名鍵K s y sを記録再生器3 0 0の内部メモリ3 0 7から読み出して、システム署名鍵K s y sをセーブデータ復号化鍵K s a vとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

次に、ステップS 7 1 5において、ステップS 7 1 4、またはステップS 7 1 7で選択、または生成されたセーブデータ復号化鍵K s a vを用いてセーブデータの復号化処理を実行し、ステップS 7 1 6において、復号したセーブデータを記録再生器3 0 0において再生、実行する。

以上で、セーブデータの再生処理が終了する。上述のようにデータ管理ファイルに「プログラム使用制限する」の設定がなされている場合は、コンテンツ固有

鍵に基づいてセーブデータ復号化鍵が生成され、「プログラム使用制限しない」の設定がある場合はシステム共通鍵に基づいてセーブデータ復号化鍵が生成される。「プログラム使用制限する」の設定がされている場合、使用しているコンテンツのコンテンツ識別子が同じものでないとセーブデータの復号処理の可能な復号化鍵を得ることができないこととなり、セーブデータのセキュリティを高めることが可能となる。

図 7 3、図 7 4 は、コンテンツ識別子を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図 7 3）、セーブデータ再生処理フロー（図 7 4）である。

図 7 3 において、ステップ S 7 2 1～S 7 2 2 は、図 7 0 のステップ S 7 0 1～S 7 0 2 と同様の処理であり、説明を省略する。

図 7 3 のセーブデータ格納処理フローは、ステップ S 7 2 2 において「プログラム使用制限する」の設定を行なった場合、ステップ S 7 2 3 においてコンテンツデータからコンテンツ識別子、すなわちコンテンツ ID を読み出してコンテンツ ID をセーブデータ暗号化鍵  $K_{sav}$  とするか、あるいはコンテンツ ID に基づいてセーブデータ暗号化鍵  $K_{sav}$  を生成する。例えば、記録再生器 3 0 0 の暗号処理部 3 0 7 はコンテンツデータから読み出したコンテンツ ID に、記録再生器 3 0 0 の内部メモリに格納されたマスター鍵  $MK_x$  を適用して、例えば DES ( $MK_x$ , コンテンツ ID) によってセーブデータ暗号化鍵  $K_{sav}$  を得ることができる。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。

一方、ステップ S 7 2 2 において、プログラム使用制限について「しない」の設定とした場合は、ステップ S 7 2 7 において、記録再生器 3 0 0 内に格納されたシステム共通鍵、例えばシステム署名鍵  $K_{sys}$  を記録再生器 3 0 0 の内部メモリ 3 0 7 から読み出して、システム署名鍵  $K_{sys}$  をセーブデータ暗号化鍵  $K_{sav}$  とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵  $K_{sav}$

a v を生成する。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。

ステップ S 724 以下の処理は、前述の図 70 の処理フローにおけるステップ S 704 以下の処理と同様であり、説明を省略する。

さらに、図 74 は、図 73 のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップ S 731 ~ S 733 は前述の図 72 の対応処理と同様であり、ステップ S 734 のみが異なる。ステップ S 734 においては、コンテンツデータからコンテンツ識別子、すなわちコンテンツ ID を読み出してコンテンツ ID をセーブデータ復号化鍵  $K_{sav}$  とするか、あるいはコンテンツ ID に基づいてセーブデータ復号化鍵  $K_{sav}$  を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ識別子に基づいて暗号化されたデータは、同一のコンテンツ識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

以下の処理、ステップ S 735、S 736、S 737 は、図 72 の対応処理と同様であるので説明を省略する。図 73、図 74 のセーブデータ格納および再生処理に従えば、プログラム使用制限するの設定を行なった場合、コンテンツ ID を使用してセーブデータ暗号化鍵、復号化鍵を生成する構成としたので、先のコンテンツ固有鍵を使用したセーブデータ格納、再生処理と同様、対応するコンテンツプログラムが整合する場合以外は、セーブデータを利用することができない構成となり、セーブデータセキュリティを高めた保存が可能となる。

図 75、図 77 は、記録再生器固有鍵を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図 75）、セーブデータ再生処理フロー（図 77）である。

図 75 において、ステップ S 741 は、図 70 のステップ S 701 と同様の処理であり、説明を省略する。ステップ S 742 は、記録再生器の制限をするかし

ないかを設定するステップである。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。ステップS 7 4 2において「記録再生器制限する」の設定をすると、ステップS 7 4 3に進み、「しない」の設定をするとステップS 7 4 7に進む。

データ管理ファイルの例を図7 6に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、記録再生器制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図6 9に示す[ I D d e v ] である。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。記録再生器制限情報は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

図7 5のセーブデータ格納処理フローにおいては、ステップS 7 4 2において「記録再生器制限する」の設定を行なった場合、ステップS 7 4 3において記録再生器3 0 0から記録再生器固有鍵、例えば記録再生器署名鍵K d e vを記録再生器3 0 0の内部メモリ3 0 7から読み出して記録再生器署名鍵K d e vをセーブデータ暗号化鍵K s a vとするか、あるいは記録再生器署名鍵K d e vに基づいてセーブデータ暗号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵K s a vとして使用してもよい。

一方、ステップS 7 4 2において、記録再生器制限について「しない」の設定とした場合は、ステップS 7 4 7において、記録再生器3 0 0内に格納されたシ

システム共通鍵、例えばシステム署名鍵  $K_{sys}$  を記録再生器 300 の内部メモリ 307 から読み出して、システム署名鍵  $K_{sys}$  をセーブデータ暗号化鍵  $K_{sav}$  とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵  $K_{sav}$  を生成する。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。

ステップ S 7 4 4、S 7 4 5 の処理は、前述の図 7 0 の処理フローにおける対応処理と同様であり、説明を省略する。

ステップ S 7 4 6 では、データ管理ファイル（図 7 6 参照）にコンテンツ識別子、記録再生器識別子、そしてステップ 7 4 2 でユーザが設定した記録再生器制限情報「する／しない」を書き込む。

さらに、図 7 7 は、図 7 5 のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップ S 7 5 1 は前述の図 7 2 の対応処理と同様、コンテンツ識別子を読み出す。次に、ステップ S 7 5 2 においては、記録再生器 300 内のメモリに格納された記録再生器識別子（ID dev）を読み出す。

ステップ S 7 5 3 では、データ管理ファイル（図 7 6 参照）からコンテンツ識別子、記録再生器識別子、設定済みの記録再生器制限情報「する／しない」の各情報を読み出す。データ管理ファイル中のコンテンツ識別子が一致するエントリにおいて、記録再生器制限情報が「する」に設定されている場合、テーブルエントリの記録再生器識別子がステップ S 7 5 2 で読み取られた記録再生器識別子と異なる場合は処理を終了する。

次に、ステップ S 7 5 4 でデータ管理ファイルの設定が「記録再生器制限する」である場合は、ステップ S 7 5 5 に進み、「しない」である場合は、ステップ S 7 5 8 に進む。

ステップ S 7 5 5 においては、記録再生器 300 から記録再生器固有鍵、例えば記録再生器署名鍵  $K_{dev}$  を記録再生器 300 の内部メモリ 307 から読み出

して記録再生器署名鍵  $K_{dev}$  をセーブデータ復号化鍵  $K_{sav}$  とするか、あるいは記録再生器署名鍵  $K_{dev}$  に基づいてセーブデータ復号化鍵  $K_{sav}$  を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器固有鍵に基づいて暗号化されたデータは、同一の記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。

一方ステップ S 758 においては、記録再生器 300 内に格納されたシステム共通鍵、例えばシステム署名鍵  $K_{sys}$  を記録再生器 300 の内部メモリ 307 から読み出して、システム署名鍵  $K_{sys}$  をセーブデータ復号化鍵  $K_{sav}$  とするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵  $K_{sav}$  を生成する。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。以下のステップ S 756, S 757 は、前述のセーブデータ再生処理フローの対応ステップと同様の処理である。

図 75、図 77 に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器固有鍵によって暗号化、復号化処理が実行されるため、同一の記録再生器固有鍵を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

次に、図 78、図 79 に記録再生器識別子を用いてセーブデータの暗号化、復号化鍵を生成して格納、再生する処理フローを示す。

図 78 は、記録再生器識別子を用いてセーブデータの暗号化を行い記録デバイスに格納する。ステップ S 761 ~ S 763 は、先の図 75 と同様の処理である。ステップ S 764 では、記録再生器から読み出した記録再生器識別子 ( $ID_{dev}$ ) を用いてセーブデータの暗号化鍵  $K_{sav}$  を生成する。 $ID_{dev}$  をセーブデータ暗号化鍵  $K_{sav}$  として適用するか、あるいは記録再生器 300 の内部

メモリに格納されたマスター鍵 $MK_x$ を適用して、 $DES(MK_x, IDdev)$ によってセーブデータ暗号化鍵 $K_{sav}$ を得る等、 $IDdev$ に基づいてセーブデータ暗号化鍵 $k_{sav}$ を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 $K_{sav}$ として使用してもよい。

以下の処理ステップS765～S768は、前述の図75の対応処理と同様であり、説明を省略する。

図79は、図78の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップS771～S774は、前述の図77の対応処理と同様である。

ステップS775では、記録再生器から読み出した記録再生器識別子( $IDdev$ )を用いてセーブデータの復号化鍵 $K_{sav}$ を生成する。 $IDdev$ をセーブデータ復号化鍵 $K_{sav}$ として適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵 $MK_x$ を適用して、 $DES(MK_x, IDdev)$ によってセーブデータ復号化鍵 $K_{sav}$ を得る等、 $IDdev$ に基づいてセーブデータ復号化鍵 $K_{sav}$ を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器識別子に基づいて暗号化されたデータは、同一の記録再生器識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 $K_{sav}$ として使用してもよい。

以下の処理ステップS776～S778は前述の図76の対応ステップの処理と同様である。

この図78、図79に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能とな

る。

次に図80～82を用いて、上述のプログラム使用制限、および記録再生器使用制限を併せて実行するセーブデータ格納、再生処理について説明する。

図80は、セーブデータ格納処理フローである。ステップS781において、コンテンツ識別子をコンテンツデータから読み出し、ステップS782において、プログラム使用制限判定を行ない、ステップS783において記録再生器制限判定を行なう。

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップS785において、コンテンツ固有鍵(ex.  $K_{con}$ )と、記録再生器固有鍵( $K_{dev}$ )の双方に基づいてセーブデータ暗号化鍵 $K_{sav}$ が生成される。これは、例えば $K_{sav} = (K_{con} \text{ XOR } K_{dev})$ 、あるいは記録再生器300の内部メモリに格納されたマスタ鍵 $MK_x$ を適用して $K_{sav} = DES(MK_x, K_{con} \text{ XOR } K_{dev})$ 等によって得ることができる。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵 $K_{sav}$ として使用してもよい。

「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップS786において、コンテンツ固有鍵(ex.  $K_{con}$ )をセーブデータ暗号化鍵 $K_{sav}$ とするか、あるいはコンテンツ固有鍵(ex.  $K_{con}$ )に基づいてセーブデータ暗号化鍵 $K_{sav}$ を生成する。

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップS787において、記録再生器固有鍵( $K_{dev}$ )をセーブデータ暗号化鍵 $K_{sav}$ とするか、あるいは記録再生器固有鍵( $K_{dev}$ )に基づいてセーブデータ暗号化鍵 $K_{sav}$ が生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵 $K_{sav}$ として使用してもよい。

さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップS787において、システム共通鍵、例えばシステム署名鍵 $K_{sys}$

をセーブデータ暗号化鍵  $K_{sav}$  とするか、あるいはシステム署名鍵  $K_{sys}$  に基づいてセーブデータ暗号化鍵  $K_{sav}$  を生成する。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。

ステップ S 789 では、ステップ S 785 ～ S 788 のいずれかで生成されたセーブデータ暗号化鍵  $K_{sav}$  によってセーブデータが暗号化され、記録デバイスに格納される。

さらに、ステップ S 790 では、ステップ S 782、S 783 において設定した制限情報がデータ管理ファイルに格納される。データ管理ファイルは、例えば図 8 1 に示す構成となり、項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限を含む。

図 8 2 は、図 8 0 の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップ S 791 では、実行プログラムのコンテンツ識別子、記録再生器識別子を読み出し、ステップ S 792 において、図 8 1 に示すデータ管理ファイルからコンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限情報を読み出す。この場合、プログラム使用制限が「する」でコンテンツ識別子が不一致である場合、または記録再生器制限情報が「する」で記録再生器識別子が不一致である場合は、処理を終了する。

次に、ステップ S 793、S 794、S 795 では、データ管理ファイルの記録データにしたがって復号鍵生成処理をステップ S 796 ～ S 799 の 4 態様のいずれかに設定する。

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップ S 796 において、コンテンツ固有鍵 (ex.  $K_{con}$ ) と、記録再生器固有鍵 ( $K_{dev}$ ) の双方に基づいてセーブデータ復号化鍵  $K_{sav}$  が生成される。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵  $K_{sav}$  として使用してもよい。「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップ S 79

7において、コンテンツ固有鍵（ex. Kcon）をセーブデータ復号化鍵Ksavとするか、あるいはコンテンツ固有鍵（ex. Kcon）に基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップS798において、記録再生器固有鍵（Kdev）をセーブデータ復号化鍵Ksavとするか、あるいは記録再生器固有鍵（Kdev）に基づいてセーブデータ復号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップS799において、システム共通鍵、例えばシステム署名鍵Ksysをセーブデータ復号化鍵Ksavとするか、あるいはシステム署名鍵Ksysに基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

これらの復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

ステップS800では、上述のステップS796～S799のいずれかにおいて生成されたセーブデータ復号化鍵を用いて復号処理が実行され、復号セーブデータが記録再生器300において再生、実行される。

この図80、82において示したセーブデータ格納、再生処理フローによれば、「プログラム使用制限する」の選択がなされたセーブデータはコンテンツ固有鍵によって暗号化、復号化処理が実行されるため、同一のコンテンツ固有鍵を持つコンテンツデータを使用する場合のみ復号して利用することが可能となる。ま

た、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。従って、コンテンツ、記録再生器両者によって利用制限を設定することが可能となり、セーブデータのセキュリティをさらに高めることが可能となる。

なお、図 8 0、8 2 においては、コンテンツ固有鍵、記録再生器固有鍵を用いたセーブデータ暗号化鍵、復号化鍵の生成構成を示したが、コンテンツ固有鍵の代わりにコンテンツ識別子、また記録再生器固有鍵の代わりに記録再生器識別子を用いて、これら識別子に基づいてセーブデータ暗号化鍵、復号化鍵の生成を実行する構成としてもよい。

次に、図 8 3～8 5 を用いてユーザの入力したパスワードに基づいてセーブデータの暗号化鍵、復号化鍵を生成する構成について説明する。

図 8 3 はユーザの入力したパスワードに基づいてセーブデータの暗号化鍵を生成して記録デバイスに格納する処理フローである。

ステップ S 8 2 1 は、コンテンツデータからコンテンツ識別子を読み出す処理であり、前述の各処理と同様である。ステップ S 8 2 2 は、ユーザによるプログラム使用制限の設定を行なうか否かを決定するステップである。本構成において設定されるデータ管理ファイルは、例えば図 8 4 に示す構成を持つ。

図 8 4 に示すように、データは、データ番号、コンテンツ識別子、記録再生器識別子、さらにユーザによるプログラム使用制限情報が含まれる。「ユーザによるプログラム使用制限情報」はプログラムを使用するユーザを制限するかしないかを設定する項目である。

図 8 3 における処理フローにおけるステップ S 8 2 2 において使用制限するの設定がなされると、ステップ S 8 2 3 においてユーザパスワードの入力がなされる。この入力、図 2 に示す例えばキーボード等の入力手段から入力される。

入力されたパスワードは、メイン CPU 1 0 6、制御部 3 0 1 の制御のもとに

暗号処理部 302 に出力され、ステップ S824 における処理、すなわち入力ユーザパスワードに基づくセーブデータ暗号化鍵  $K_{sav}$  が生成される。セーブデータ暗号化鍵  $K_{sav}$  生成処理としては、例えばパスワード自体を暗号化鍵  $K_{sav}$  としてもよいし、あるいは記録再生器のマスタ鍵  $MK_x$  を用いて、セーブデータ暗号化鍵  $K_{sav} = DES(MK_x, \text{パスワード})$  によって生成してもよい。また、パスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵を生成してもよい。

ステップ S822 におけるユーザ制限が No とされている場合は、ステップ S828 において、記録再生器 300 のシステム共通鍵に基づいてセーブデータ暗号化鍵が生成される。

さらに、ステップ S825 でステップ S824、またはステップ S828 で生成したセーブデータ暗号化鍵  $K_{sav}$  を用いてセーブデータの暗号化処理がなされ、ステップ S826 において暗号化処理のなされたセーブデータが記録デバイスに格納される。

さらに、ステップ S827 において、図 84 のデータ管理ファイルにステップ S822 で設定したユーザによるプログラム使用制限情報が、コンテンツ識別子と記録再生器識別子に対応付けられて書き込まれる。

図 85 は、図 83 の処理によって格納されたセーブデータの再生処理フローを示した図である。ステップ S831 において、コンテンツデータからコンテンツ識別子を読み出し、ステップ S832 において図 84 に示したデータ管理ファイルからコンテンツ識別子、ユーザによるプログラム使用制限情報を読み出す。

ステップ S833 において、データ管理ファイル中のデータに基づく判定を実行し、「ユーザによるプログラム使用制限する」が設定されている場合は、ステップ S834 において、パスワード入力を求め、ステップ S835 において、入力パスワードに基づく復号化鍵を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるパスワードに基づいて暗号化されたデータは、同一のパスワードに基づいて生成された復号鍵によって復

号可能なものとなる復号化鍵生成アルゴリズムに設定される。

ステップS 8 3 3の判定がユーザによるプログラム使用制限なしの場合は、ステップS 8 3 7において記録再生器3 0 0の内部メモリに格納されたシステム共通鍵、例えばシステム署名鍵K s y sを用いてセーブデータ復号鍵K s a vが生成される。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

ステップS 8 3 6では、ステップS 8 3 5、ステップS 8 3 7のいずれかにおいて生成された復号化鍵K s a vを用いて記録デバイスに格納されたセーブデータの復号が実行され、ステップS 8 3 6において記録再生器においてセーブデータの再生、実行がなされる。

図8 3、図8 5において示したセーブデータ格納、再生処理フローによれば、「ユーザによるプログラム使用制限する」の選択がなされたセーブデータはユーザ入力パスワードに基づく鍵によって暗号化、復号化処理が実行されるため、同一のパスワードを入力した場合のみ復号して利用することが可能となり、セーブデータのセキュリティを高めることが可能となる。

以上、いくつかのセーブデータの格納処理、再生処理態様について説明してきたが、上述した処理を融合した処理、例えばパスワードと、記録再生器識別子、コンテンツ識別子等を任意に組み合わせて使用してセーブデータ暗号化鍵、復号化鍵を生成する態様も可能である。

#### (1 7) 不正機器の排除（リボケーション）構成

すでに説明してきたように、本発明のデータ処理装置においては、メディア5 0 0（図3参照）、通信手段6 0 0から提供される様々なコンテンツデータを記録再生器3 0 0において、認証、暗号化処理等を実行し、記録デバイスに格納する構成によって提供コンテンツのセキュリティを高めるとともに、また、正当な利用者のみが利用可能とする構成を持つ。

上述の説明から理解されるように、入力コンテンツは、記録再生器3 0 0の暗

号処理部 302 に構成される内部メモリ 307 に格納された様々な署名鍵、マスター鍵、チェック値生成鍵（図 18 参照）を用いて、認証処理、暗号化处理、復号化处理がなされる。この鍵情報を格納する内部メモリ 307 は、先に説明したように、基本的に外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされるのが望ましいが、万が一内部メモリの不正な読み取りが実行され、これらの鍵データ等が流出し、正規なライセンスのされていない記録再生器にコピーされた場合、コピーされた鍵情報によって不正なコンテンツ利用がなされる可能性がある。

ここでは、これらの不正コピーによる鍵の複製によるコンテンツの不正利用を防止する構成について説明する。

図 86 に、本構成「(17) 不正機器の排除構成」を説明するブロック図を示す。記録再生器 300 は、前述の図 2, 3 に示す記録再生器と同様であり、内部メモリを有し、先に説明した（図 18）各種の鍵データ、さらに、記録再生器識別子を有している。なお、ここでは、第三者によって複製されている記録再生器識別子、鍵データ等は図 3 に示す内部メモリ 307 に格納されるとは限らず、図 86 に示す記録再生器 300 の鍵データ等は、暗号処理部 302（図 2, 3 参照）によってアクセス可能なメモリ部にまとめて、あるいは分散して格納されている構成であるとする。

不正機器の排除構成を実現するため、コンテンツデータのヘッダ部の不正な記録再生器識別子リストを記憶した構成とした。図 86 に示すように、コンテンツデータには、不正な記録再生器識別子（IDdev）リストとしてのリボケーション（Revocation）リストを保有している。さらに、リボケーションリストの改竄チェック用のリストチェック値 ICVrev を設けている。不正な記録再生器識別子（IDdev）リストは、コンテンツ提供者、または管理者が、例えば不正コピーの流通状態等から判明した不正な記録再生器の識別子 IDdev

vをリスト化したものである。このリボケーションリストは例えば配送鍵K d i sによって暗号化されて格納してもよい。記録再生器による復号処理については、例えば先の図22のコンテンツダウンロード処理の態様と同様である。

なお、ここでは、理解を容易にするため、リボケーションリストを単独のデータとして図86のコンテンツデータ中に示してあるが、例えば先に説明したコンテンツデータのヘッダ部の構成要素である取扱方針（例えば図32～35参照）中にリボケーションリストを含ませてもよい。この場合は、先に説明したチェック値I C V aによってリボケーションリストを含む取扱方針データの改竄チェックがなされる。リボケーションリストが取扱方針中に含まれる場合は、チェック値A：I C V aのチェックによって代替され、記録再生器内のチェック値A生成鍵K i c v aが利用され、チェック値生成鍵K i c v - r e vを格納する必要はない。

リボケーションリストを単独のデータとしてコンテンツデータ中に含ませる場合は、リボケーションリストの改竄チェック用のリストチェック値I C V r e vによるリボケーションリストのチェックを実行するとともに、リストチェック値I C V r e vとコンテンツデータ中の他の部分チェック値とから中間チェック値を生成して中間チェック値の検証処理を行なう構成とする。

リボケーションリストの改竄チェック用のリストチェック値I C V r e vによるリボケーションリストのチェック手法は、前述の図23、図24等で説明したI C V a、I C V b等のチェック値生成処理と同様の方法で実行可能である。すなわち、記録再生器暗号処理部302の内部メモリ307に保存したチェック値生成鍵K i c v - r e vを鍵とし、コンテンツデータ中に含まれるリボケーションリストをメッセージとして図23、図24等で説明したI C V計算方法に従って計算される。計算したチェック値I C V - r e v' とヘッダ（Header）内に格納されたチェック値：I C V - r e vを比較し、一致していた場合には、改竄が無いと判定する。

リストチェック値I C V r e vを含む中間チェック値は、例えば、図25に示

すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されている総チェック値生成鍵  $K_{icvt}$  を鍵とし、検証した  $Header$  内のチェック値  $A$ 、チェック値  $B$ 、リストチェック値  $ICV_{rev}$ 、さらにフォーマットに応じてコンテンツチェック値を加えたメッセージ列に図 7 他で説明した  $ICV$  計算方法を適用して生成する。

これらのリボケーションリスト、リストチェック値は、DVD、CD等のメディア 500、通信手段 600 を介して、あるいはメモリカード等の記録デバイス 400 を介して記録再生器 300 に提供される。ここで記録再生器 300 は、正当な鍵データを保有する記録再生器である場合と、不正に複製された識別子  $ID$  を有する場合とがある。

このような構成における不正な記録再生器の排除処理の処理フローを図 87 および図 88 に示す。図 87 は、DVD、CD等のメディア 500、あるいは通信手段 600 からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローであり、図 88 は、メモリカード等の記録デバイス 400 からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローである。

まず、図 87 の処理フローについて説明する。ステップ 901 は、メディアを装着して、コンテンツの提供、すなわち再生処理あるいはダウンロードの要求を行なうステップである。この図 87 に示す処理は、例えば記録再生器に DVD 等のメディアを装着してダウンロード処理等を実行する前のステップとして実行される。ダウンロード処理については、先に図 22 を用いて説明している通りであり、図 22 の処理フローの実行の前ステップとして、あるいは図 22 の処理フロー中に挿入される処理としてこの図 87 の処理が実行される。

記録再生器 300 がネットワーク等の通信手段を介してコンテンツ提供を受ける場合は、ステップ S911 においてコンテンツ配信サービス側との通信セッションを確立し、その後、ステップ S902 へ進む。

ステップ S902 では、コンテンツデータのヘッダ部からリボケーションリス

ト(図86参照)を取得する。このリスト取得処理は、コンテンツがメディア内にある場合は、図3に示す制御部301が読取部304を介してメディアから読み出し、コンテンツが通信手段からである場合は、図3に示す制御部301が通信部305を介してコンテンツ配信側から受信する。

次にステップS903において、制御部301は、暗号処理部302にメディア500または通信手段600から取得したリボケーションリストを暗号処理部302に渡し、チェック値生成処理を実行させる。記録再生器300は、内部にリボケーションチェック値生成鍵 $K_{icv-rev}$ を有し、受領したリボケーションリストをメッセージとしてリボケーションチェック値生成鍵 $K_{icv-rev}$ を適用して、例えば図23、図24等で説明したICV計算方法に従ってチェック値 $ICV-rev'$ を計算し、計算結果とコンテンツデータのヘッダ(Header)内に格納されたチェック値: $ICV-rev$ を比較し、一致していた場合には改竄が無い(ステップS904でYes)と判定する。一致しない場合は、改竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。

次に、ステップS905において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に総チェック値 $ICVt'$ の計算をさせる。総チェック値 $ICVt'$ は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵 $K_{sys}$ を鍵とし、中間チェック値をDESで暗号化して生成する。なお、各部分チェック値、例えば $ICVa$ 、 $ICVb$ 等の検証処理は、この図87に示す処理フロー中では省略してあるが、先に説明した図39～図45の処理フローと同様の各データフォーマットに応じた部分チェック値の検証が行なわれる。

次に、ステップS906において、生成した総チェック値 $ICVt'$ とヘッダ(Header)内の $ICVt$ を比較し、一致していた場合(ステップS906でYes)には、ステップS907へ進む。一致しない場合は、改竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。

先に説明したように、総チェック値  $ICV_t$  は、 $ICV_a$ 、 $ICV_b$ 、さらに、データフォーマットに応じて各コンテンツブロックのチェック値等、コンテンツデータに含まれる部分チェック値全体をチェックするものであるが、ここでは、これらの部分チェック値にさらに、リボケーションリストの改竄チェック用のリストチェック値  $ICV_{rev}$  を部分チェック値として加えて、これら全ての改竄を検証する。上述の処理によって生成された総チェック値がヘッダ (Header) 内に格納されたチェック値： $ICV_t$  と一致した場合には、 $ICV_a$ 、 $ICV_b$ 、各コンテンツブロックのチェック値、およびリストチェック値  $ICV_{rev}$  全ての改竄はないと判断される。

さらにステップ S 9 0 7 では、改竄無しと判定されたリボケーションリストと、自己の記録再生器 3 0 0 に格納された記録再生器識別子 ( $ID_{dev}$ ) との比較がなされる。

コンテンツデータから読み出された不正な記録再生器識別子  $ID_{dev}$  のリストに自己の記録再生器の識別子  $ID_{dev}$  が含まれている場合は、その記録再生器 3 0 0 は、不正に複製された鍵データを有していると判定され、ステップ S 9 0 9 に進み、以後の手続きは中止される。例えば図 2 2 のコンテンツダウンロード処理の手続きの実行を不可能とする。

ステップ S 9 0 7 において、不正な記録再生器識別子  $ID_{dev}$  のリストに自己の記録再生器の識別子  $ID_{dev}$  が含まれていないと判定された場合には、その記録再生器 3 0 0 は、正当な鍵データを有していると判定され、ステップ S 9 0 8 に進み、以後の手続き、例えば、プログラム実行処理、あるいは図 2 2 等のコンテンツダウンロード処理等が実行可能となる。

図 8 8 は、メモ리카ード等の記録デバイス 4 0 0 に格納したコンテンツデータを再生する場合の処理を示す。先に説明したように、メモ리카ード等の記録デバイス 4 0 0 と記録再生器 3 0 0 は、図 2 0 で説明した相互認証処理 (ステップ S 9 2 1) が実行される。ステップ S 9 2 2 において、相互認証 OK である場合にのみ、ステップ S 9 2 3 以降の処理に進み、相互認証に失敗した場合は、ステップ

S 9 3 0のエラーとなり、以降の処理は実行されない。

ステップS 9 2 3では、コンテンツデータのヘッダ部からリボケーションリスト(図8 6参照)を取得する。以降のステップS 9 2 4～S 9 3 0の処理は、先の図8 7における対応処理と同様の処理である。すなわち、リストチェック値によるリストの検証(S 9 2 4, S 9 2 5)、総チェック値による検証(S 9 2 6, S 9 2 7)、リストのエントリと自己の記録再生器識別子ID d e vとの比較(S 9 2 8)を実行し、コンテンツデータから読み出された不正な記録再生器識別子ID d e vのリストに自己の記録再生器の識別子ID d e vが含まれている場合は、その記録再生器3 0 0は、不正に複製された鍵データを有していると判定され、ステップS 9 3 0に進み、以後の手続きは中止される。例えば図2 8に示すコンテンツの再生処理を実行不可能とする。一方、不正な記録再生器識別子ID d e vのリストに自己の記録再生器の識別子ID d e vが含まれていないと判定された場合には、その記録再生器3 0 0は、正当な鍵データを有していると判定され、ステップS 9 2 9に進み、以後の手続きが実行可能となる。

このように、本発明のデータ処理装置においては、コンテンツ提供者、または管理者が提供するコンテンツに併せて不正な記録再生器を識別するデータ、すなわち不正な記録再生器識別子ID d e vをリスト化したリボケーションリストをコンテンツデータのヘッダ部の構成データとして含ませて記録再生器利用者に提供し、記録再生器利用者は、記録再生器によるコンテンツの利用に先立って、自己の記録再生器のメモリに格納された記録再生器識別子ID d e vと、リストの識別子との照合を実行して一致するデータが存在した場合には、以後の処理を実行させない構成としたので鍵データを複製してメモリに格納した不正な記録再生器によるコンテンツ利用を排除することが可能となる。

#### (1 8) セキュアチップ構成および製造方法

先に説明したように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7、あるいは記録デバイス4 0 0の内部メモリ4 0 5は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従っ

て、記録再生器暗号処理部 3 0 2、記録デバイス暗号処理部 4 0 1 は、例えば外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

しかしながら、上述の説明で理解されるように、例えば記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 には記録再生器署名鍵 *K d e v* 等の記録再生器毎に異なるデータを書き込むことが必要となる。また、チップ内の不揮発性の記憶領域、例えばフラッシュメモリ、*F e R A M* 等にチップ毎の個別情報、例えば識別情報 (*I D*) や暗号鍵情報を書き込んだ後、例えば製品出荷後におけるデータの再書き込み、読み出しを困難とすることが必要となる。

従来の書き込みデータの読み出し、再書き込み処理を困難とするための手法には、例えばデータ書き込みのコマンドプロトコルを秘密にする。あるいは、チップ上のデータ書き込みコマンドを受け付ける信号線と、製品化した後に利用される通信用の信号線を分離して構成し、基板上のチップに直接信号を送らない限りデータ書き込みコマンドが有効とならないようにする等の手法がある。

しかしながら、このような従来手法を採用しても、記憶素子の専門知識を有するものにとっては、回路を駆動させる設備と技術があれば、チップのデータ書き込み領域に対する信号出力が可能であり、また、たとえデータ書き込みのコマンドプロトコルが秘密であったとしても、プロトコルの解析可能性は常に存在する。

このような、秘密データの改変可能性を保持した暗号処理データの格納素子を流通させることは、暗号処理システム全体を脅かす結果となる。また、データの読み出しを防止するために、データ読み出しコマンド自体を実装しない構成とすることも可能であるが、その場合、正規のデータ書き込みを実行した場合であっても、メモリに対するデータ書き込みが実際に行われたか否かを確認したり、書き込まれたデータが正確に書き込まれているか否かを判定することが不可能とな

り、不良なデータ書き込みの行われたチップが供給される可能性が発生する。

これらの従来技術に鑑み、ここでは、例えばフラッシュメモリ、F e R A M等の不揮発性メモリに正確なデータ書き込みを可能とするとともに、データの読み出しを困難にするセキュアチップ構成およびセキュアチップ製造方法を提供する。

図89に、例えば、前述の記録再生器暗号処理部302または記録デバイス400の暗号処理部401に適用可能なセキュリティチップ構成を示す。図89(A)はチップの製造過程、すなわちデータの書き込み過程におけるセキュリティチップ構成を示し、図89(B)は、データを書き込んだセキュリティチップを搭載した製品の構成例、例えば記録再生器300、記録デバイス400の例を示す。

製造過程にあるセキュリティチップは、処理部8001にモード指定用信号線8003、および各種コマンド信号線8004が接続され、処理部8001は、モード指定用信号線8003で設定されたモード、例えばデータ書き込みモードまたはデータ読み出しモードに応じて不揮発性メモリである記憶部8002へのデータ書き込み処理、または記憶部8002からのデータ読み出し処理を実行する。

一方、図89(B)のセキュリティチップ搭載製品においては、セキュリティチップと外部接続インタフェース、周辺機器、他の素子等とが汎用信号線で接続されるが、モード信号線8003は、非接続状態とされる。具体的な処理は、例えばモード信号線8003をグランド接続する、V c cに釣り上げる、信号線をカットする、あるいは絶縁体樹脂で封印する等である。このような処理により、製品出荷後は、セキュリティチップのモード信号線に対するアクセスが困難になり、外部からチップのデータを読み出したり書き込みを行なったりすることの困難性を高めることができる。

さらに、本構成のセキュリティチップ8000は、データの記憶部8002に対する書き込み処理、および記憶部8002に書き込まれたデータの読み出し処

理を困難にする構成を持ち、たとえ第三者がモード信号線 8003 のアクセスに成功した場合であっても不正なデータ書き込み、読み出しを防止可能である。図 90 に本構成を有するセキュリティチップにおけるデータ書き込みまたは読み出し処理フローを示す。

ステップ S 9 5 1 は、モード信号線 8003 をデータ書き込みモードまたはデータ読み出しモードに設定するステップである。

ステップ S 9 5 2 は、チップから認証用情報を取り出すステップである。本構成のセキュリティチップには、例えばワイヤ (Wire)、マスク ROM 構成により、予めパスワード、暗号技術における認証処理用の鍵情報等、認証処理に必要な情報が格納される。ステップ S 9 5 2 は、この認証情報を読み出して認証処理を実行する。例えば正規なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証 OK (ステップ S 9 5 3 において Yes) の結果が得られるが、不正なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証に失敗 (ステップ S 9 5 3 において No) し、その時点で処理が中止される。認証処理は、例えば先に説明した図 13 の相互認証処理手続きに従って実行可能である。図 89 に示す処理部 8001 は、これらの認証処理を実行可能な構成を有する。これは、例えば先に説明した図 29 に示す記録デバイス 400 の暗号処理部 401 の制御部 403 に組み込まれたコマンドレジスタと同様の構成により実現可能である。例えば図 89 のチップの処理部は、図 29 に示す記録デバイス 400 の暗号処理部 401 の制御部 403 に組み込まれたコマンドレジスタと同様の構成を持ち、各種コマンド信号線 8004 に接続された機器から所定のコマンド No が入力されると、対応する処理を実行し、認証処理シーケンスを実行することが可能となる。

処理部 8001 は認証処理において認証がなされた場合にのみ、データの書き込みコマンド、またはデータの読み出しコマンドを受け付けてデータの書き込み処理 (ステップ S 9 5 5)、またはデータの読み出し処理 (ステップ S 9 5 6)

を実行する。

このように本構成のセキュリティチップにおいては、データの書き込み時、読み出し時に認証処理を実行する構成としたので、正当な権利を持たない第三者によるセキュリティチップの記憶部からデータの読み出し、または記憶部へのデータ書き込みを防止することができる。

次に、さらに、セキュリティの高い素子構成とした実施例を図 9 1 に示す。この例では、セキュリティチップの記憶部 8 2 0 0 が 2 つの領域に分離され、一方はデータの読み書きが可能な読み出し書き込み併用領域 (RW: ReadWrite 領域) 8 2 0 1 であり、他方はデータの書き込みのみが可能な書き込み専用領域 (WO: WriteOnly 領域) 8 2 0 2 である。

この構成において、書き込み専用領域 (WO: WriteOnly 領域) 8 2 0 2 には、暗号鍵データ、識別子データ等のセキュリティ要請の高いデータを書き込み、一方セキュリティ度のさほど高くない、例えばチェック用のデータ等を読み出し書き込み併用領域 (RW: ReadWrite 領域) 8 2 0 1 に書き込む。

処理部 8 0 0 1 は、読み出し書き込み併用領域 (RW: ReadWrite 領域) 8 2 0 1 からのデータ読み出し処理は、前述の図 9 0 で説明した認証処理を伴うデータ読み出し処理を実行する。しかし、データ書き込み処理は、図 9 2 のフローに従って実行する。

図 9 2 のステップ S 9 6 1 は、モード信号線 8 0 0 3 を書き込みモードに設定するステップであり、ステップ 9 6 2 では、先の図 9 0 で説明したと同様の認証処理を実行する。認証処理で認証がなされると、ステップ S 9 6 3 に進み、コマンド信号線 8 0 0 4 を介して、書き込み専用 (WO) 領域 8 2 0 2 にセキュリティの高い鍵データ等の情報の書き込み、読み出し書き込み併用領域 (RW: ReadWrite 領域) 8 2 0 1 にセキュリティ度のさほど高くない、例えばチェック用データ書き込むコマンドを処理部 8 0 0 1 に対して出力する。

ステップ S 9 6 4 ではコマンドを受領した処理部 8 0 0 1 が、コマンドに応じ

たデータ書き込み処理をそれぞれ書き込み専用（WO）領域 8202、読み出し書き込み併用領域（RW：Read Write 領域）8201に対して実行する。

また、書き込み専用（WO）領域 8202に書き込まれたデータの検証処理フローを図 93 に示す。

図 93 のステップ S971 は、処理部 8001 において、書き込み専用（WO）領域 8202 に書き込まれたデータに基づく暗号処理を実行させる。これらの実行構成は、先の認証処理実行構成と同様、コマンドレジスタに格納された暗号処理シーケンスを順次実行する構成によって実現される。また、処理部 8001 において実行される暗号処理アルゴリズムは特に限定されるものではなく、例えば先に説明した DES アルゴリズムを実行する構成とすることができる。

次に、ステップ S972 で、セキュリティチップに接続された検証装置が処理部 8001 から暗号処理結果を受信する。次に、ステップ S973 において、先に記憶部に書き込み処理を行なった正規な書き込みデータに対して処理部 8001 において実行されたアルゴリズムと同様の暗号化処理を適用して得た結果と、処理部 8001 からの暗号化結果とを比較する。

比較した結果が同一であれば、書き込み専用（WO）領域 8202 に書き込まれたデータは正しいことが検証される。

この構成では、認証処理が破られて読み出しコマンドが万が一実行可能となっても、データの読み出し可能領域は、読み出し書き込み併用領域（RW：Read Write 領域）8201 に限定され、書き込み専用（WO）領域 8202 に書き込まれたデータの読み出しは、不可能であり、さらにセキュリティの高い構成となる。また、全く読み出しを不可能としたチップと異なり、読み出し書き込み併用領域（RW：Read Write 領域）8201 が構成されているのでメモリアクセスの正否チェックが可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであ

り、限定的に解釈されるべきではない。また、上記した実施例ではコンテンツの記録、再生を可能な記録再生器を例にして説明してきたが、データ記録のみ、データ再生のみ可能な装置においても本発明の構成は適用可能なものであり、本発明はパーソナルコンピュータ、ゲーム機器、その他の各種データ処理装置一般において実施可能なものである。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

#### 産業上の利用の可能性

本発明は、DVD、CD等の記憶媒体、あるいはCATV、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモ리카ード、ハードディスク、CD-R等に格納するとともに、記録デバイスに格納されたコンテンツを利用する際、コンテンツ配信側の希望する利用制限を付す構成を実現するとともに、この配布されたコンテンツを、正規ユーザ以外の第三者に不正利用されないようにセキュリティを確保する装置及びシステムに利用できる。

## 請 求 の 範 囲

1. 相互に暗号データの転送を実行する記録再生器と記録デバイスとからなるデータ処理システムにおいて、

上記記録デバイスは、

記録再生器と記録デバイス間において転送可能なコンテンツデータを記憶するデータ記憶部を有するとともに、

記録再生器と記録デバイス間の少なくとも認証処理に適用可能な鍵データを格納した鍵ブロックを複数有し、該複数の鍵ブロックに格納された鍵データは各ブロック毎に異なる鍵データを格納した構成を持ち、

上記記録再生器は、

記録再生器と記録デバイス間の認証処理において、上記記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して、指定鍵ブロックに格納された鍵データに基づいて上記記録デバイスとの認証処理を実行する構成を有することを特徴とするデータ処理システム。

2. 上記記録デバイスの複数の鍵ブロック各々には、少なくとも認証処理に適用可能な認証鍵を含み、各鍵ブロックの認証鍵は相互に異なる鍵データとして構成されていることを特徴とする請求の範囲第1項に記載のデータ処理システム。

3. 上記記録再生器は、

認証処理に適用すべき鍵ブロックを指定鍵ブロックとして設定した設定情報を記録再生器内メモリに保持し、

上記記録再生器は、

記録再生器と記録デバイス間の認証処理に際して記録再生器内メモリに保持された設定情報に基づいて上記記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して認証処理を実行する構成であることを特徴とする請求の範

図第 1 項に記載のデータ処理システム。

4. 上記記録再生器の指定鍵ブロック設定情報は、記録再生器の機種またはバージョンまたは出荷先等の所定製品単位毎に異なるように設定された構成であることを特徴とする請求の範囲第 3 項に記載のデータ処理システム。

5. 上記記録再生器は、

上記記録デバイスとの認証処理に必要な認証処理用鍵データを記録再生器内メモリに格納した構成を持ち、

上記記録再生器内メモリに格納された認証処理用鍵データは、上記記録デバイスの複数の鍵ブロックの一部の鍵ブロックにのみ格納されたブロック内鍵データを使用した認証処理においてのみ認証が成立し、他の鍵ブロック内鍵データを用いた認証処理においては認証の成立しない鍵データであることを特徴とする請求の範囲第 1 項に記載のデータ処理システム。

6. 上記記録再生器は、

記録デバイス認証鍵用マスター鍵MKakeを記録再生器内メモリに格納し、  
上記記録デバイス認証鍵用マスター鍵MKakeに基づいて生成される認証鍵Kakeは、該記録再生器に設定された指定鍵ブロック内の鍵データを使用した認証処理においてのみ認証が成立し、他の鍵ブロック内鍵データを用いた認証処理においては認証の成立しない認証鍵であることを特徴とする請求の範囲第 1 項に記載のデータ処理システム。

7. 上記記録デバイスは、上記記録デバイス内メモリに記録デバイス識別情報IDmemを有するとともに、上記複数の鍵ブロックの各々に鍵ブロック毎に異なる認証鍵Kakeを格納した構成を有し、

上記記録再生器は、

記録再生器内メモリに格納された記録デバイス認証鍵用マスター鍵MKakeに基づく上記記録デバイス識別情報IDmemの暗号処理によって認証鍵Kakeを生成し、該生成した認証鍵Kakeを用いて上記記録デバイスの指定鍵ブロックとの認証処理を行なう構成を有することを特徴とする請求の範囲第6項に記載のデータ処理システム。

8. 上記記録デバイスの鍵ブロックの各々には、記録デバイスの固有情報である記録デバイス識別子情報、記録再生器間との認証処理において使用される認証鍵および乱数生成鍵、さらに上記データ記憶部への格納データの暗号化処理に用いられる保存鍵を含むことを特徴とする請求の範囲第1項に記載のデータ処理システム。

9. 上記記録デバイスの複数の鍵ブロックの各々に格納された上記保存鍵は、各鍵ブロック毎に異なる鍵データであるとともに上記データ記憶部の格納データに対する暗号処理に用いられる鍵であり、

上記記録デバイスは、

記録デバイス外部から保存鍵で暗号化されたデータの利用要求があった場合は、記録デバイス内において保存鍵の鍵交換処理を実行して保存鍵と異なる鍵による暗号化データを記録デバイス外部に出力する構成を有することを特徴とする請求の範囲第8項に記載のデータ処理システム。

10. 上記記録デバイスは、暗号処理部を有し、

該暗号処理部は、

上記記録再生器から受信する鍵ブロック指定情報に従って記録デバイスの複数の鍵ブロックの1つの鍵ブロックを選択し、該選択鍵ブロック内の鍵データを用いて上記記録再生器との認証処理を実行する構成を有することを特徴とする請求の範囲第1項に記載のデータ処理システム。

1 1. 上記記録デバイスにおける暗号処理部は、

記録再生器と記録デバイス間において転送可能なコンテンツデータを記憶したデータ記憶部に対するデータ格納処理およびデータ記憶部からのデータ転送処理において実行する暗号処理を上記記録再生器から受信する鍵ブロック指定情報に従って選択した1つの鍵ブロック内の鍵データを用いて実行する構成を有することを特徴とする請求の範囲第10項に記載のデータ処理システム。

1 2. 上記記録再生器の指定可能な上記記録デバイスの鍵ブロックは複数であり、該複数の指定可能な鍵ブロック中の少なくとも1つの鍵ブロックは、他の記録再生器においても指定可能な共通指定可能な鍵ブロックとして構成されていることを特徴とする請求の範囲第1項に記載のデータ処理システム。

1 3. 外部装置との間で転送可能なコンテンツデータを記憶するデータ記憶部を有する記録デバイスであり、

記録デバイスと上記外部装置間の少なくとも認証処理に適用可能な鍵データを格納した鍵ブロックを複数有し、該複数の鍵ブロックに格納された鍵データは各ブロック毎に異なる鍵データを格納した構成を有することを特徴とする記録デバイス。

1 4. 上記記録デバイスの複数の鍵ブロック各々には、少なくとも認証処理に適用可能な認証鍵を含み、各鍵ブロックの認証鍵は相互に異なる鍵データとして構成されていることを特徴とする請求の範囲第13項に記載の記録デバイス。

1 5. 上記記録デバイスは、

上記記録デバイス内メモリに記録デバイス識別情報IDmemを有するとともに、上記複数の鍵ブロックの各々に鍵ブロック毎に異なる認証鍵Kakeを格納

した構成を有することを特徴とする請求の範囲第 13 項に記載の記録デバイス。

16. 上記記録デバイスの鍵ブロックの各々には、記録デバイスの固有情報である記録デバイス識別子情報、上記外部装置との認証処理において使用される認証鍵および乱数生成鍵、さらに上記データ記憶部への格納データの暗号化処理に用いられる保存鍵を含むことを特徴とする請求の範囲第 13 項に記載の記録デバイス。

17. 上記記録デバイスの複数の鍵ブロックの各々に格納された上記保存鍵は、各鍵ブロック毎に異なる鍵データであるとともに上記データ記憶部の格納データに対する暗号処理に用いられる鍵であり、

上記記録デバイスは、

記録デバイス外部から保存鍵で暗号化されたデータの利用要求があった場合は、記録デバイス内において保存鍵の鍵交換処理を実行して保存鍵と異なる鍵による暗号化データを記録デバイス外部に出力する構成を有することを特徴とする請求の範囲第 16 項に記載の記録デバイス。

18. 上記記録デバイスは、暗号処理部を有し、

該暗号処理部は、

上記外部装置から受信する鍵ブロック指定情報に従って記録デバイスの複数の鍵ブロックの 1 つの鍵ブロックを選択し、該選択鍵ブロック内の鍵データを用いて上記記録再生器との認証処理を実行する構成を有することを特徴とする請求の範囲第 13 項に記載の記録デバイス。

19. 上記記録デバイスにおける暗号処理部は、

上記外部装置と記録デバイス間において転送可能なコンテンツデータを記憶したデータ記憶部に対するデータ格納処理およびデータ記憶部からのデータ転送処

理において実行する暗号処理を上記外部装置から受信する鍵ブロック指定情報に従って選択した1つの鍵ブロック内の鍵データを用いて実行する構成を有することを特徴とする請求の範囲第18項に記載の記録デバイス。

20. 相互に暗号データの転送を実行する記録再生器と記録デバイスとからなるデータ処理システムにおけるデータ処理方法において、

記録再生器が、記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して、指定鍵ブロックに格納された鍵データに基づいて上記記録デバイスとの認証処理を実行することを特徴とするデータ処理方法。

21. 上記記録デバイスの複数の鍵ブロック各々には、少なくとも認証処理に適用可能な認証鍵を含み、各鍵ブロックの認証鍵は相互に異なる鍵データとして構成されていることを特徴とする請求の範囲第20項に記載のデータ処理方法。

22. 上記データ処理方法において、

上記記録再生器は、記録再生器と記録デバイス間の認証処理に際して記録再生器内メモリに保持された設定情報に基づいて上記記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して認証処理を実行することを特徴とする請求の範囲第20項に記載のデータ処理方法。

23. 上記データ処理方法において、

上記記録再生器は、記録デバイス認証鍵用マスター鍵MKakeを記録再生器内メモリに格納し、

上記記録デバイス認証鍵用マスター鍵MKakeに基づいて認証鍵Kakeを生成し、

生成した認証鍵Kakeを用いて上記記録デバイスの有する複数の鍵ブロック中の指定鍵ブロック内の鍵データを使用した認証処理を実行することを特徴とす

る請求の範囲第20項に記載のデータ処理方法。

24. 上記データ処理方法において、

上記記録デバイスは、上記記録デバイス内メモリに記録デバイス識別情報IDmemを有するとともに、上記複数の鍵ブロックの各々に鍵ブロック毎に異なる認証鍵Kakeを格納した構成を有し、

上記記録再生器は、記録再生器内メモリに格納された記録デバイス認証鍵用マスター鍵MKakeに基づく上記記録デバイス識別情報IDmemの暗号処理を実行して認証鍵Kakeを生成し、

生成した認証鍵Kakeを用いて上記記録デバイスの指定鍵ブロックとの認証処理を行なうことを特徴とする請求の範囲第20項に記載のデータ処理方法。

25. 上記データ処理方法において、

上記記録デバイスは、上記記録再生器から受信する鍵ブロック指定情報に従って記録デバイスの複数の鍵ブロックの1つの鍵ブロックを選択し、該選択鍵ブロック内の鍵データを用いて上記記録再生器との認証処理を実行することを特徴とする請求の範囲第20項に記載のデータ処理方法。

26. 上記データ処理方法において、

上記記録デバイスは、記録再生器と記録デバイス間において転送可能なコンテンツデータを記憶したデータ記憶部に対するデータ格納処理およびデータ記憶部からのデータ転送処理において実行する暗号処理を上記記録再生器から受信する鍵ブロック指定情報に従って選択した1つの鍵ブロック内の鍵データを用いて実行することを特徴とする請求の範囲第20項に記載のデータ処理方法。

27. 上記データ処理方法において、

上記記録デバイスの複数の鍵ブロックの各々には、上記記録デバイス内のデー

タ記憶部の格納データの暗号処理に用いられる保存鍵を含み、

記録デバイス外部から保存鍵で暗号化されたデータの利用要求があった場合、記録デバイス内において保存鍵の鍵交換処理を実行して保存鍵と異なる鍵による暗号化データを記録デバイス外部に出力することを特徴とする請求の範囲第20項に記載のデータ処理方法。

28. 相互に暗号データの転送を実行する記録再生器と記録デバイスとからなるデータ処理システムにおけるデータ処理方法をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、記録再生器が、記録デバイスの有する複数の鍵ブロックから1つの鍵ブロックを指定して、指定鍵ブロックに格納された鍵データに基づいて上記記録デバイスとの認証処理を実行するステップを含むことを特徴とするプログラム提供媒体。

29. 相互に暗号データの転送を実行する第1の装置と第2の装置とからなるデータ処理システムにおいて、

上記第2の装置は、上記第1の装置との転送データに関する暗号処理を実行する暗号処理部を有し、

該暗号処理部は、

上記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、

該制御部は、上記第1の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とするデータ処理システム。

30. 上記制御部の有する上記第1の装置から受領するコマンド識別子に関する

設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、

上記制御部は、上記第 1 の装置からの受領コマンド番号の受付値をメモリに格納するとともに、上記第 1 の装置からの新規受領コマンド番号を、上記メモリに格納した受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行わず、上記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする請求の範囲第 29 項に記載のデータ処理システム。

31. 上記第 2 の装置は、上記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、

上記コマンドレジスタには、

上記第 1 の装置と上記第 2 の装置との認証処理を実行する認証処理コマンドシーケンスと、

上記第 1 の装置と上記第 2 の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、

上記認証処理コマンドシーケンスに対応するコマンド識別子は、上記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする請求の範囲第 29 項に記載のデータ処理システム。

32. 上記暗号処理コマンドシーケンスは、

上記第 1 の装置から上記第 2 の装置に対して転送され、上記第 2 の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、

上記第 2 の装置内の記憶手段に格納され、上記第 2 の装置から上記第 1 の装置

に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、

少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする請求の範囲第 3 1 項に記載のデータ処理システム。

### 3 3. 上記制御部は、

上記第 1 の装置と上記第 2 の装置との認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、上記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、

上記制御部は、

上記認証処理コマンドシーケンスを新たに実行する際に上記認証フラグをリセットすることを特徴とする請求の範囲第 3 1 項に記載のデータ処理システム。

### 3 4. 上記制御部は、

上記暗号鍵交換処理において、上記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

上記制御部は、上記鍵交換処理に関する一連のコマンド実行中は、上記第 1 の装置を含む外部装置からの上記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする請求の範囲第 3 2 項に記載のデータ処理システム。

### 3 5. 上記第 2 の装置は、暗号化データを記憶するデータ記憶部を有する記憶デバイスであり、

上記第 1 の装置は、上記記憶デバイスに対するデータの格納処理、および上記記憶デバイスに格納されたデータを取り出して再生、実行を行なう記録再生器であり、

上記記録再生器は、上記記録デバイスとの転送データの暗号処理を実行する暗号処理部を有することを特徴とする請求の範囲第29項に記載のデータ処理システム。

36. 上記記録デバイスは、

上記記録再生器と記録デバイス間の認証処理に適用する認証鍵、および上記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、

上記記録デバイスの暗号処理部における上記制御部は、

上記記録再生器から上記設定シーケンスにしたがってコマンド識別子を受領して上記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に上記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする請求の範囲第35項に記載のデータ処理システム。

37. 上記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、

上記記録再生器は、上記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する1つの鍵ブロックを指定鍵ブロックとして上記記録デバイスに通知し、上記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする請求の範囲第36項に記載のデータ処理システム。

38. 外部装置との間で転送可能なコンテンツデータを記憶するデータ記憶部を有する記録デバイスであり、

上記記録デバイスは、外部装置との転送データに関する暗号処理を実行する暗号処理部を有し、

該暗号処理部は、

外部装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させる制御部を有し、

該制御部は、上記外部装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止する構成を有することを特徴とする記録デバイス。

39. 上記制御部は、上記設定シーケンスとして、順次、番号がインクリメントされるコマンド番号設定シーケンスを有し、

上記制御部は、上記外部装置からの受領コマンド番号の受付値をメモリに格納するとともに、上記外部装置からの新規受領コマンド番号を、上記メモリに格納した受付済みコマンド番号に基づいて設定シーケンスとの一致を判定し、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行わず、上記メモリに格納したコマンド番号のリセットを実行する構成を有することを特徴とする請求の範囲第38項に記載の記録デバイス。

40. 上記記録デバイスは、上記設定シーケンスに従ったコマンドを格納したコマンドレジスタを有し、

上記コマンドレジスタには、

上記外部装置と上記記録デバイスとの認証処理を実行する認証処理コマンドシーケンスと、

上記外部装置と上記記録デバイスとの間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとが格納されており、

上記認証処理コマンドシーケンスに対応するコマンド識別子は、上記暗号処理コマンドシーケンスに対応するコマンド識別子より以前のステップにおいて実行されるようにシーケンス設定がなされていることを特徴とする請求の範囲第38項に記載の記録デバイス。

#### 4 1. 上記暗号処理コマンドシーケンスは、

上記外部装置から上記記録デバイスに対して転送され、上記記録デバイス内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、

上記記録デバイス内の記憶手段に格納され、上記記録デバイスから上記外部装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、

少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする請求の範囲第40項に記載の記録デバイス。

#### 4 2. 上記制御部は、

上記外部装置と上記記録デバイスとの認証処理により認証が成立した場合に、認証済みであることを示す認証フラグを設定し、該認証フラグが設定されている間は、上記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行し、

上記制御部は、

上記認証処理コマンドシーケンスを新たに実行する際に上記認証フラグをリセットすることを特徴とする請求の範囲第40項に記載の記録デバイス。

#### 4 3. 上記制御部は、

上記暗号鍵交換処理において、上記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

上記制御部は、上記鍵交換処理に関する一連のコマンド実行中は、上記外部装置を含む外部装置からの上記設定シーケンスと異なるコマンド処理を受け付けない構成であることを特徴とする請求の範囲第41項に記載の記録デバイス。

#### 44. 上記記録デバイスは、

上記外部装置と記録デバイス間の認証処理に適用する認証鍵、および上記記録デバイス内のデータ記憶部に格納するデータの暗号化鍵としての保存鍵を格納した鍵ブロックを有し、

上記記録デバイスの暗号処理部における上記制御部は、

上記外部装置から上記設定シーケンスにしたがってコマンド識別子を受領して上記鍵ブロックに格納した認証鍵を用いた認証処理を実行し、該認証処理完了後に上記保存鍵を用いた鍵交換処理を伴うデータの暗号処理を実行する構成であることを特徴とする請求の範囲第38項に記載の記録デバイス。

#### 45. 上記鍵ブロックは、それぞれ異なる認証鍵および保存鍵を格納した複数の鍵ブロックから構成され、

上記外部装置は、上記複数の鍵ブロックから、認証処理およびデータの暗号処理に使用する1つの鍵ブロックを指定鍵ブロックとして上記記録デバイスに通知し、上記記録デバイスは、指定鍵ブロックに格納された認証鍵を用いた認証処理、および保存鍵を用いたデータの暗号処理を実行する構成であることを特徴とする請求の範囲第44項に記載の記録デバイス。

#### 46. 相互に暗号データの転送を実行する第1の装置と第2の装置とからなるデータ処理システムにおけるデータ処理方法であり、

上記第2の装置は、

上記第1の装置から転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを実行し、

上記コマンド処理制御において、上記第1の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止することを特徴とするデータ処理方法。

47. 上記コマンド処理制御ステップにおいて、上記第1の装置から受領するコマンド識別子に関する設定シーケンスは、順次、番号がインクリメントされるコマンド番号設定シーケンスであり、

上記コマンド処理制御ステップは、

上記第1の装置からの受領コマンド番号の受付値をメモリに格納するステップと、

上記第1の装置からの新規受領コマンド番号を、上記メモリに格納した受付済みコマンド番号に基づいて設定シーケンスとの一致を判定する判定ステップと、

上記判定ステップにおいて、設定シーケンスと異なると判定された場合には、該新規受領コマンド番号に対応するコマンド処理を行わず、上記メモリに格納したコマンド番号のリセットを実行することを特徴とする請求の範囲第46項に記載のデータ処理方法。

48. 上記データ処理方法において、

上記コマンド処理制御ステップは、

上記第1の装置と上記第2の装置との認証処理を実行する認証処理コマンドシーケンスと、

上記第1の装置と上記第2の装置との間における転送データに関する暗号処理を実行する暗号処理コマンドシーケンスとを、

実行するステップであり、

上記設定シーケンスは、上記認証処理コマンドシーケンスを上記暗号処理コマンドシーケンスに先行して実行するシーケンスであることを特徴とする請求の範囲第46項に記載のデータ処理方法。

49. 上記データ処理方法において、

上記暗号処理コマンドシーケンスは、

上記第 1 の装置から上記第 2 の装置に対して転送され、上記第 2 の装置内の記憶手段に格納される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、または、

上記第 2 の装置内の記憶手段に格納され、上記第 2 の装置から上記第 1 の装置に対して転送される暗号化データに対する暗号鍵交換処理を含むコマンドシーケンス、

少なくとも上記いずれかのコマンドシーケンスを含むことを特徴とする請求の範囲第 4 8 項に記載のデータ処理方法。

50. 上記データ処理方法において、

上記第 1 の装置と上記第 2 の装置との認証処理により認証が成立した場合に認証済みであることを示す認証フラグを設定する認証フラグ設定ステップを含み、

上記コマンド処理制御ステップは、

上記認証フラグが設定されている間は、上記暗号処理コマンドシーケンスの実行を可能とするコマンド管理制御を実行することを特徴とする請求の範囲第 4 8 項に記載のデータ処理方法。

51. 上記データ処理方法において、

上記認証処理コマンドシーケンスを新たに実行する際に上記認証フラグをリセットすることを特徴とする請求の範囲第 50 項に記載のデータ処理方法。

52. 上記データ処理方法における上記コマンド処理制御ステップにおいて、

上記鍵交換処理に関する一連のコマンド実行中は、上記設定シーケンスおよびコマンド識別子に基づいてコマンド実行順序を管理し、

上記第 1 の装置を含む外部装置からの上記設定シーケンスと異なるコマンド処理を受け付けないことを特徴とする請求の範囲第 49 項に記載のデータ処理方法。

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00526

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.<sup>7</sup> H04L9/32, H04L9/08, G09C1/00, G06F12/14, G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.<sup>7</sup> H04L9/32, H04L9/08, G09C1/00, G06F12/14, G06F9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001  
 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-65662, A (Sony Corporation), 06 March, 1998 (06.03.98), Par. Nos. [0034] to [0035], [0052]; Par. Nos. [0071] to [0072]; Figs. 1 to 13 & US, 5883958, A	1-27
Y	JP, 10-327142, A (Sony Corporation), 08 December, 1998 (08.12.98), Par. Nos. [0002] to [0006]; Fig. 20 & EP, 867843, A & US, 6058477, A	1-27, 37, 45
Y	JP, 6-289782, A (Matsushita Electric Ind. Co., Ltd.), 18 October, 1994 (18.10.94), Par. Nos. [0014] to [0015]; Fig. 1 (Family: none)	6, 7, 23, 24
Y	JP, 11-306088, A (Toppan Printing Co., Ltd.), 05 November, 1999 (05.11.99), Full text; all drawings (Family: none)	29-52

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
17 April, 2001 (17.04.01)Date of mailing of the international search report  
01 May, 2001 (01.05.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00526

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-179951, A (Dainippon Printing Co., Ltd.), 11 July, 1997 (11.07.97), Par. No. [0017]; Fig. 3 (Family: none)	29-52
Y	JP, 11-355265, A (Matsushita Electric Ind. Co., Ltd.), 24 December, 1999 (24.12.99), Par. No. [0053]; page 8, Column 14, lines 38 to 43; page 8, Column 14, line 48 to page 9, Column 15, line 1 & WO, 99/050992, A & EP, 994599, A & CN, 1266572, T	36,44
Y	JP, 11-185006, A (Dainippon Printing Co., Ltd.), 09 July, 1999 (09.07.99) Full text; all drawings (Family: none)	33,42,50

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00526

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 28,53  
because they relate to subject matter not required to be searched by this Authority, namely:  
  
The inventions of claims 28, 53 relate to a program. However no hardware resources are used for expression, they relate to a program source. Therefore the subject matter relates to mere presentation of information and is not required to be searched by this International Searching Authority according to PCT Article 17(2)(a)(i) and Rule 39.1(v).
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-27 relate to the functional structures of a data processing system for performing authentication between a recording/reproducing device and a recording device by designating a key block out of different items of key data stored in key blocks, a storage device, and a data processing method. The inventions of claims 29-52 relate to the processing by a second device for a command identifier transmitted from a first device. These groups of inventions relate to functional structures of different gists. Therefore the group of inventions 1-27 and the group of inventions 29-52 do not fulfill the requirement of unity of invention.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

**THIS PAGE BLANK (USPTO)**

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/32, H04L9/08, G09C1/00, G06F12/14,  
G06F9/06

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/32, H04L9/08, G09C1/00, G06F12/14,  
G06F9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年  
日本国公開実用新案公報 1971-2001年  
日本国登録実用新案公報 1994-2001年  
日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 10-65662, A (ソニー株式会社) 6. 3月. 1998 (06. 03. 98) 第【0034】-【0035】段落, 第【0052】段落, 第【0071】-【0072】段落, 図1-13 & US, 5883958, A	1-27
Y	J P, 10-327142, A (ソニー株式会社) 8. 12月. 1998 (08. 12. 98) 第【0002】-【0006】段落, 図20 & EP, 867843, A & US, 6058477, A	1-27, 37, 45

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

17. 04. 01

国際調査報告の発送日

01.05.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 6-289782, A (松下電器産業株式会社) 18. 10月. 1994 (18. 10. 94) 第【0014】-【0015】段落, 図1 (ファミリーなし)	6, 7, 23, 24
Y	JP, 11-306088, A (凸版印刷株式会社) 5. 11月. 1999 (05. 11. 99) 全文, 全図 (ファミリーなし)	29-52
Y	JP, 9-179951, A (大日本印刷株式会社) 11. 7月. 1997 (11. 07. 97) 第【0017】段落, 図3 (ファミリーなし)	29-52
Y	JP, 11-355265, A (松下電器産業株式会社) 24. 12月. 1999 (24. 12. 99) 第【0053】段落, 第8頁第14欄第38-43行, 第8頁第14欄第48行-第9頁第15欄第1行 & WO, 99050992, A & EP, 994599, A & CN, 1266572, T	36, 44
Y	JP11-185006, A (大日本印刷株式会社) 9. 7月. 1999 (09. 07. 99) 全文, 全図 (ファミリーなし)	33, 42, 50



**THIS PAGE BLANK (USPTO)**